



Cisco Lean Retail Oracle E-Business Suite 11i Application Deployment Guide

Cisco Validated Design

April 14, 2008

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-16515-01

Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)



CONTENTS

Introduction	1-1
Scope	1-2
Enterprise Architecture	1-2
Enterprise Application Overview	1-3
Desktop Tier	1-4
Application Tier	1-5
Database Tier	1-6
Enterprise Network Architecture	1-6
Data Center Network Components	1-6
Store Network Components	1-9
Technology Overview	1-10
Application Control Engine	1-11
Firewall Services Module	1-15
Wide Area Application Engine	1-15
Design and Implementation Details	1-17
Design Goals	1-17
Design Implementation	1-17
Store Designs	1-17
ACE Routed Mode Design	1-20
Performance Observations	1-36
Summary and Conclusions	1-39
Appendix A—Configurations	1-39
ACE Configuration	1-39
ACE Admin Context	1-39
ACE Oracle11i Context	1-40
WAE Configuration	1-44
Appendix B—References	1-45
Appendix C—Glossary	1-46



Cisco Lean Retail Oracle E-Business Suite 11i Application Deployment Guide

This document provides network design best practices to enhance an Oracle E-Business Suite 11i application environment across the WAN. It introduces key concepts and options regarding the application deployment and detailed designs strategies available to a data center leveraging Cisco application and networking technologies.

Introduction

The Cisco Lean Retail Oracle E-Business Suite solution provides best practices and implementation guidance that optimizes application availability, performance, and security while lowering application ownership costs. Cisco's Lean Retail architecture provides accelerated application performance and improved access to information. Data center-based applications and hosted managed services can have their performance accelerated to LAN-like speeds. The Oracle E-Business Suite is an extensive set of business applications developed to assist enterprises in addressing these challenges. The E-Business application framework is a flexible environment designed to protect, extend, and evolve business processes.

Cisco's Lean Retail architecture includes:

- Application and collaboration services
- Integrated networking services
- Reference network designs

A key Lean Retail integrated network service is the Application Networking Service (ANS). This solution focuses on the ANS components of Cisco Application Control Engine (ACE) and Wide Area Application Services (WAAS) product families. It provides data center, retail store, and remote end-user application optimization services. This solution addresses the following Oracle E-Business Suite deployment challenges:

- Reduced capital and operational costs for applications, servers, and networking
- Recovery time objectives (RTO) and recovery point objectives (RPO) for business continuity
- Application response time over limited WAN connections
- Application, server, network, and service-oriented architecture (SOA) security



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

The value of Cisco's Lean Retail is accomplished through four key benefits:

- **Application availability**—When an application server fails in a store, only that store is impacted. When an application fails in a data center, many stores are impacted. A core tenet of Cisco's Lean Retail is the centralization of application services. Through server virtualization and load balancing, greater application uptime is achieved. Virtualized server resources in the data center leverage clustering and load balancing to share and distribute load across a larger pool of resources. A single failure does not impact overall accessibility of the application users.
- **Performance improvement**—Traditionally, retailers use low bandwidth links. Many retailers have hundreds to thousands of stores. The incremental addition of WAN bandwidth per store significantly increases OPEX costs due to economies of scale. Retailers get more for less through the use of virtualized servers, load balancing, and WAAS. Performance is significantly improved for the end user (both in stores and across the Web). Servers are more fully utilized when loads are balanced across larger clusters. WAN performance is improved by locally caching content and accelerating the TCP protocol.
- **Increased security**—Retailers need to comply with industry and regulatory requirements (e.g., PCI, HIPPA, and SOX to avoid fines and penalties). Security features including encryption, segmentation, and authentication address many of these requirements. Cisco ACE applies stateful inspection rules that explicitly allow or deny specified traffic patterns. Cisco ACE also uses role-based access control to give independent access to both security and load-balancing policies. The Cisco ACE XML Gateway provides a full Layer 7 proxy and includes integrated XML security for Web services transactions.
- **Lowering application ownership costs**—Many retailers have hundreds to thousands of stores. Typically they have several servers in each store. For both existing and new applications, the incremental costs per store are significant. By removing servers from the stores, retailers are able to reduce OPEX costs on average of 16%¹.

Deploying new applications and capabilities quickly and effectively are key IT metrics that improve an organization's business agility. Cisco's Lean Retail enables more applications to be deployed centrally, cutting down dramatically on the time and cost of deployment. Deploying centrally also reduces the costs of opening new stores and of integrating acquisitions. While many retailers will choose to deploy some applications in the stores, Lean Retail Architecture improves the capabilities of a central deployment model. To learn more about Cisco's Lean Retail, see:

<http://www.cisco.com/web/strategy/retail/lean-retail.html>

Scope

Cisco data center and store architectures are established enterprise designs that deliver highly available and robust network infrastructures. This document describes the deployment of the Oracle E-Business Suite in a Cisco data center while leveraging services available in the store. This end-to-end solution design employs many integrated network services, including load balancing, security, and application optimization.

Enterprise Architecture

This section describes the application architecture of the Oracle E-Business Suite 11i.

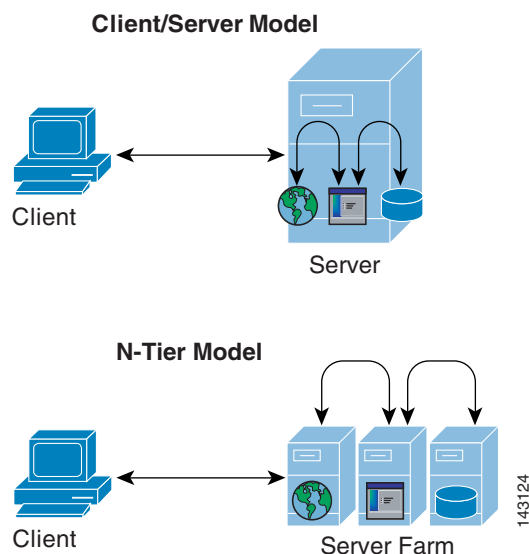
1. Gartner: Server consolidation can save money 12/2005.

Enterprise Application Overview

The data center is a repository for enterprise software applications that are continuously changing to meet business requirements and to accommodate the latest technological advances and methods. Consequently, the logical and physical structure of the data center server farm and of the network infrastructure hosting these software applications is also continuously changing.

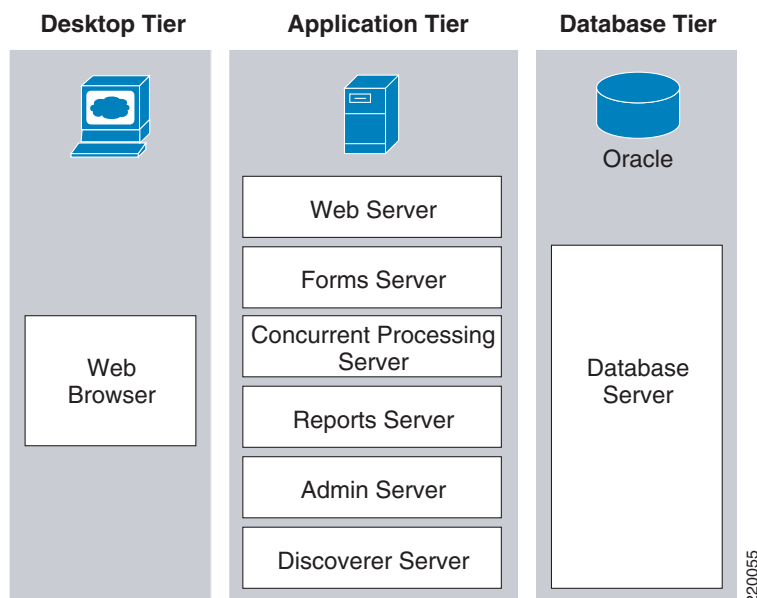
The server farm has evolved from the classic client/server model to an N-tier approach, where “N” implies any number, such as 2-tier, or 4-tier; basically, any number of distinct tiers used in the architecture. The N-tier model logically or physically separates the enterprise application by creating functional areas. These areas are generally defined as the web front end, the application business logic, and the database tiers. [Figure 1](#) shows the progression of the enterprise application from the client/server to N-tier paradigm.

Figure 1 *Client/Server and N-Tier Model*



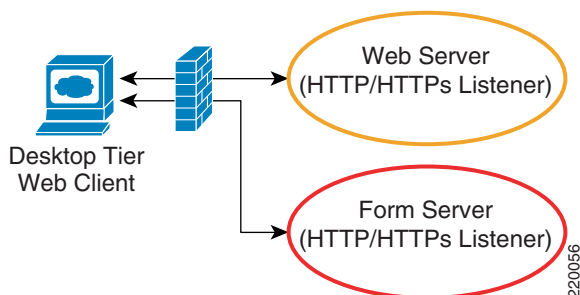
The N-tier model provides a more scalable and manageable enterprise application environment because it creates distinct serviceable areas in the software application. The application is distributed and becomes more resilient as single points of failure are removed from the design.

The Oracle Application Architecture uses the N-tier model by distributing application services across nodes in the server farm. The Oracle Application Architecture, as shown in [Figure 2](#), uses the logical separation of tiers as desktop, application, and database. It is important to remember that each tier can consist of one or more physical hosts to provide the enterprise with the required performance or application availability.

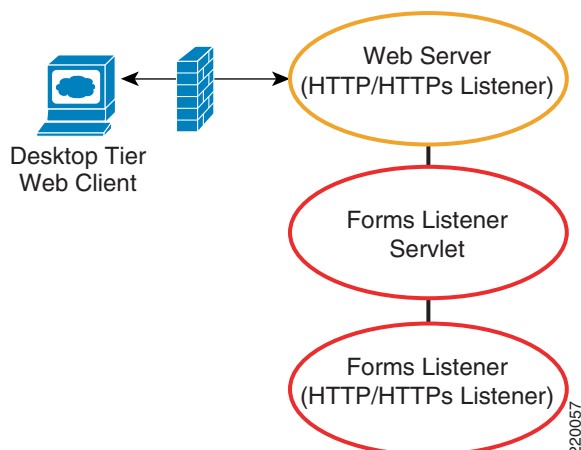
Figure 2 *Oracle Application Architectures*

Desktop Tier

The desktop tier, traditionally called the presentation layer, consists of the store user interface (a web browser). The browser connects to the application tier via HTTP or HTTPS to the web server or the forms server. Historically, the forms server required the use of a client-side applet, Oracle JInitiator, which runs as an Active-X or plug-in on the client browser using a direct socket connection to the forms server. This direct-connect environment requires the associate to access the forms server directly. This obviously exposes an enterprise to potential security risks when connectivity is allowed beyond the confines of the corporate LAN or WAN by requiring “holes” in firewalls. [Figure 3](#) shows the impact of a direct socket connection on the firewall and the security of the enterprise.

Figure 3 *Traditional Desktop to Form Server Connections*

In 2002, Oracle E-Business Suite offered a more “Internet-friendly” forms server application by allowing a Java forms listener servlet to intercept forms server requests via the web listener. The forms listener servlet allows a single HTTP or HTTPS connection between the client, desktop tier, and the application tier. [Figure 4](#) shows the more secure forms listener servlet deployment model, which can also take advantage of standard SSL offload and load balancing approaches.

Figure 4 Forms Listener Servlet Architecture**Note**

The forms listener servlet deployment model is now common in enterprise data centers. The remainder of this document assumes the use of this forms strategy.

Application Tier

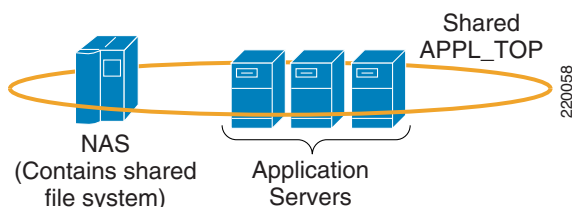
The application tier of the Oracle E-Business Suite provides administrative services and business logic, allowing end users at the desktop tier to make use of the information found at the database tier. [Figure 2](#) shows the primary servers residing in this layer:

- Web server
- Forms server
- Concurrent processing server
- Admin server
- Reports server
- Discoverer server

Each of the application servers provides business process logic or management services to the Oracle E-Business Suite-enabled enterprise. The desktop tier communicates with the application tier via the web server listener (see [Figure 4](#)).

The application tier is commonly referred to as the APPL_TOP. The APPL_TOP is a file system that can reside on a single physical node or span multiple nodes in a “shared” multi-node application tier deployment. A shared APPL_TOP resides on a common disk mounted by each node in the 11i installation. A shared APPL_TOP allows any of the nodes to invoke the six primary server functions, such as the web server and forms server. The primary advantage to a shared application tier deployment is the ability to patch and/or modify a single file system in a multi-node deployment, propagating those changes to all nodes simultaneously.

In addition, the use of a single file system requires the backup of only a single file system despite the use of multiple nodes. [Figure 5](#) shows three server nodes sharing the application file system via NFS. The shared mount point in this case is a storage device located in the network.

Figure 5 Shared Application File System**Note**

Windows systems do not support a shared application tier in an Oracle 11i environment. For more information on shared application tier file systems, see Oracle Metalink Document 243880.1.

Database Tier

A database is a structured collection of data. This complex construct consists of tables, indexes, and stored procedures; each an important element to organize and access the data. Oracle provides a database management system (DBMS) or relational DBMS (RDBMS) to interface with the data collected by the application tier. The database tier does not directly communicate with the desktop tier; instead, the database relies on the application tier as an intermediary. To provide increased performance, scalability, and availability, Oracle offers Real Application Clusters (RAC), which allow multiple nodes to support a single database instance.

**Note**

For more information on Oracle applications, see “Oracle Applications Concepts Release 11i” part number B19295-02 at <http://www.oracle.com>.

Enterprise Network Architecture

Data Center Network Components

The logical topology of the data center infrastructure can be divided into the front-end network and the back-end network, depending on their role:

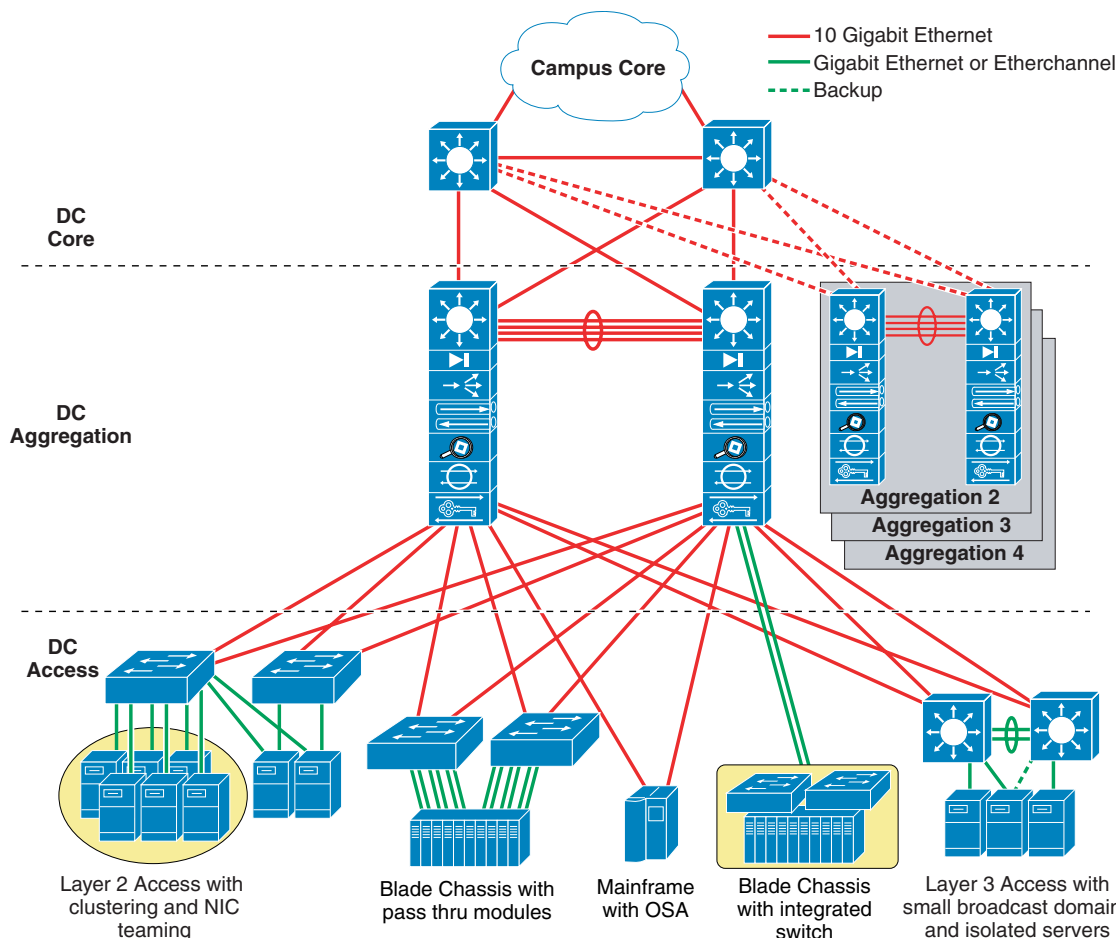
- The front-end network provides the IP routing and switching environment, including client-to-server, server-to-server, and server-to-storage network connectivity.
- The back-end network supports the storage area network (SAN) fabric and connectivity between servers and other storage devices, such as storage arrays and tape drives.

Front-End Network

The front-end network contains three distinct functional layers:

- Core
- Aggregation
- Access

Figure 6 shows a multi-tier front-end network topology and a variety of services that are available at each of these layers.

Figure 6 Data Center Multi-Tier Model Topology

143311

Core Layer

The core layer is a gateway that provides high-speed connectivity to external entities such as the WAN, intranet, and extranet of the campus. The data center core is a Layer 3 domain where efficient forwarding of packets is the fundamental objective. To this end, the data center core is built with high-bandwidth links (10 GE) and employs routing best practices to optimize traffic flows.

Aggregation Layer

The aggregation layer is a point of convergence for network traffic that provides connectivity between server farms at the access layer and the rest of the enterprise. The aggregation layer supports Layer 2 and Layer 3 functionality, and is an ideal location for deploying centralized application, security, and management services. These data center services are shared across the access layer server farms, and provide common services in a way that is efficient, scalable, predictable, and deterministic.

The aggregation layer provides a comprehensive set of features for the data center. The following devices support these features:

- Multilayer aggregation switches
- Load balancing devices
- Firewalls

- Wide area application acceleration
- Intrusion detection systems
- Content engines
- Secure Sockets Layer (SSL) offloaders
- Network analysis devices

Access Layer

The primary role of the access layer is to provide the server farms with the required port density. In addition, the access layer must be a flexible, efficient, and predictable environment to support client-to-server and server-to-server traffic. A Layer 2 domain meets these requirements by providing the following:

- Layer 2 adjacency between servers and service devices
- A deterministic, fast converging, loop-free topology

Layer 2 adjacency in the server farm lets you deploy servers or clusters that require the exchange of information at Layer 2 only. It also readily supports access to network services in the aggregation layer, such as load balancers and firewalls. This enables an efficient use of shared, centralized network services by the server farms.

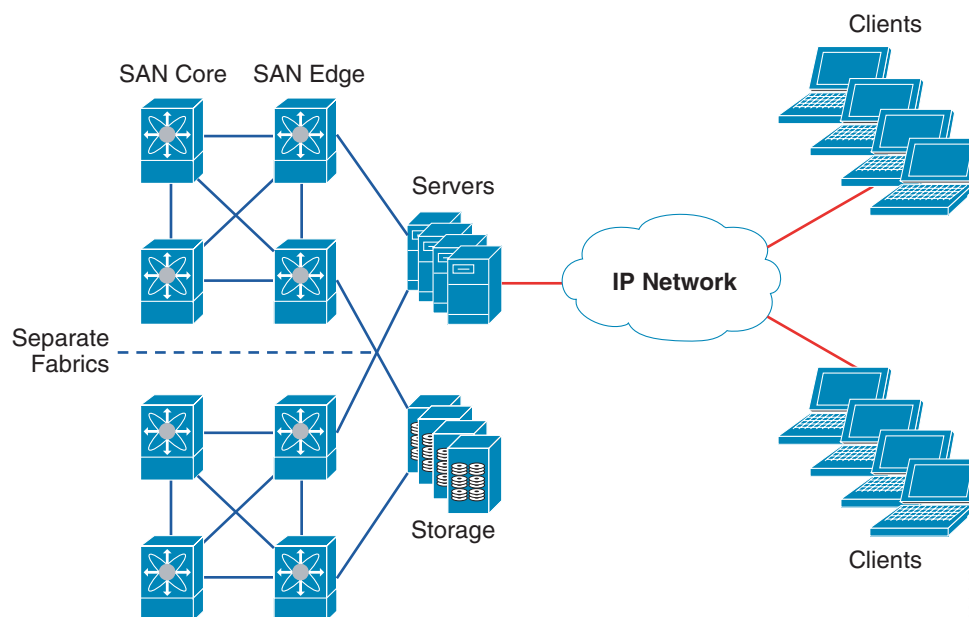
In contrast, if services are deployed at each access switch, the benefit of those services is limited to the servers directly attached to the switch. Through access at Layer 2, it is easier to insert new servers into the access layer. The aggregation layer is responsible for data center services, while the Layer 2 environment focuses on supporting scalable port density.

Layer 3 access designs are not widely deployed in current data centers. However, to minimize fault domains and provide rapid convergence, network administrators are seeking to leverage the benefits of Layer 3. Layer 3 designs do not exclude the introduction of network services, but the transparency of the service at the aggregation layer is more difficult to maintain. As with all access layer designs, the requirements of the application environments drive the decision for either model. The access layer must provide a deterministic environment to ensure a stable Layer 2 domain regardless of its size. A predictable access layer allows spanning tree to converge and recover quickly during failover and fallback.

Back-End Network

The back-end SAN consists of core and edge SAN storage layers to facilitate high-speed data transfers between hosts and storage devices. SAN designs are based on the FiberChannel (FC) protocol. Speed, data integrity, and high availability are key requirements in an FC network. In some cases, in-order delivery must be guaranteed. Traditional routing protocols are not necessary on FC. Fabric Shortest Path First (FSFP), similar to OSPF, runs on all switches for fast fabric convergence and best path selection. Redundant components are present from the hosts to the switches and to the storage devices. Multiple paths exist and are in use between the storage devices and the hosts. Completely separate physical fabrics are a common practice to guard against control plane instability, ensuring high availability in the event of any single component failure.

Figure 7 shows the SAN topology.

Figure 7 SAN Topology**SAN Core Layer**

The SAN core layer provides high-speed connectivity to the edge switches and external connections. Connectivity between core and edge switches are 10 Gbps links or trunking of multiple full rate links for maximum throughput. Core switches also act as master devices for selected management functions, such as the primary zoning switch and Cisco fabric services. In addition, advanced storage functions such as virtualization, continuous data protection, and iSCSI reside in the SAN core layer.

SAN Edge Layer

The SAN edge layer is analogous to the access layer in an IP network. End devices such as hosts, storage, and tape devices connect to the SAN edge layer. Compared to IP networks, SANs are much smaller in scale, but the SAN must still accommodate connectivity from all hosts and storage devices in the data center. Over-subscription and planned core-to-edge fan out ratio result in high port density on SAN switches. On larger SAN installations, it is common to segregate the storage devices to additional edge switches.

**Note**

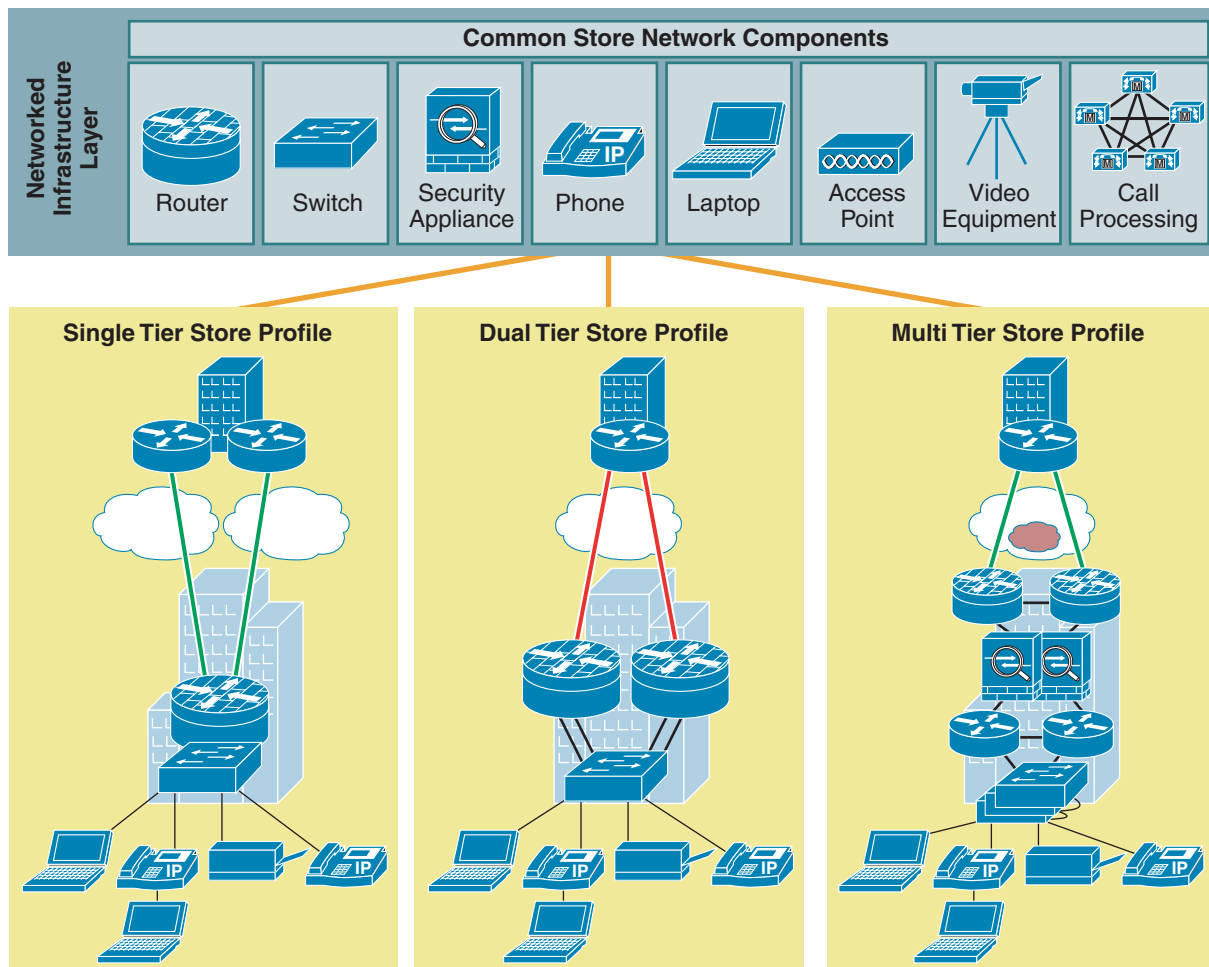
For more information on Cisco data center designs or other places in the network, see the following URL: <http://www.cisco.com/go/srnd>.

Store Network Components

The store network provides users connectivity to corporate resources such as the centralized application services residing in the enterprise data center. The architectural design of the store varies depending on the availability, scalability, security, and other service requirements of the organization.

The Cisco enterprise branch architecture framework defines the network infrastructure, network services, and application optimization capabilities of three typical branch deployment models used in typical store designs. Figure 8 shows these three common store solutions. Each of these profiles provides varying degrees of scalability and resiliency in addition to integrated network and application services.

Figure 8 **Network Infrastructure Layer — Three Models**



Technology Overview

This section provides an overview of the significant Cisco products and technologies leveraged in this design. The following products are addressed:

- Cisco Application Control Engine (ACE)
- Cisco Firewall Services Module (FWSM)
- Cisco Wide Area Application Engine (WAE)

Application Control Engine

Overview

The Cisco Application Control Engine (ACE) provides a highly available and scalable data center solution from which the Oracle E-Business Suite application environment may benefit. Currently, the ACE is available as an appliance or integrated service module in the Catalyst 6500 platform. ACE features and benefits include the following:

- Device partitioning (up to 250 virtual ACE contexts)
- Load balancing services (up to 16 Gbps of throughput capacity, 345,000 L4 connections/second)
- Security services via deep packet inspection, access control lists (ACLs), unicast reverse path forwarding (URPF), Network Address Translation (NAT)/Port Address Translation (PAT) with fix-ups, syslog, and so on
- Centralized role-based management via Application Network Manager (ANM) GUI or CLI
- SSL Offload (up to 15,000 SSL sessions via licensing)
- Support for redundant configurations (intra-chassis, inter-chassis, inter-context)

The following sections describe some of the features and functionalities employed in the Oracle E-Business Suite application environment.

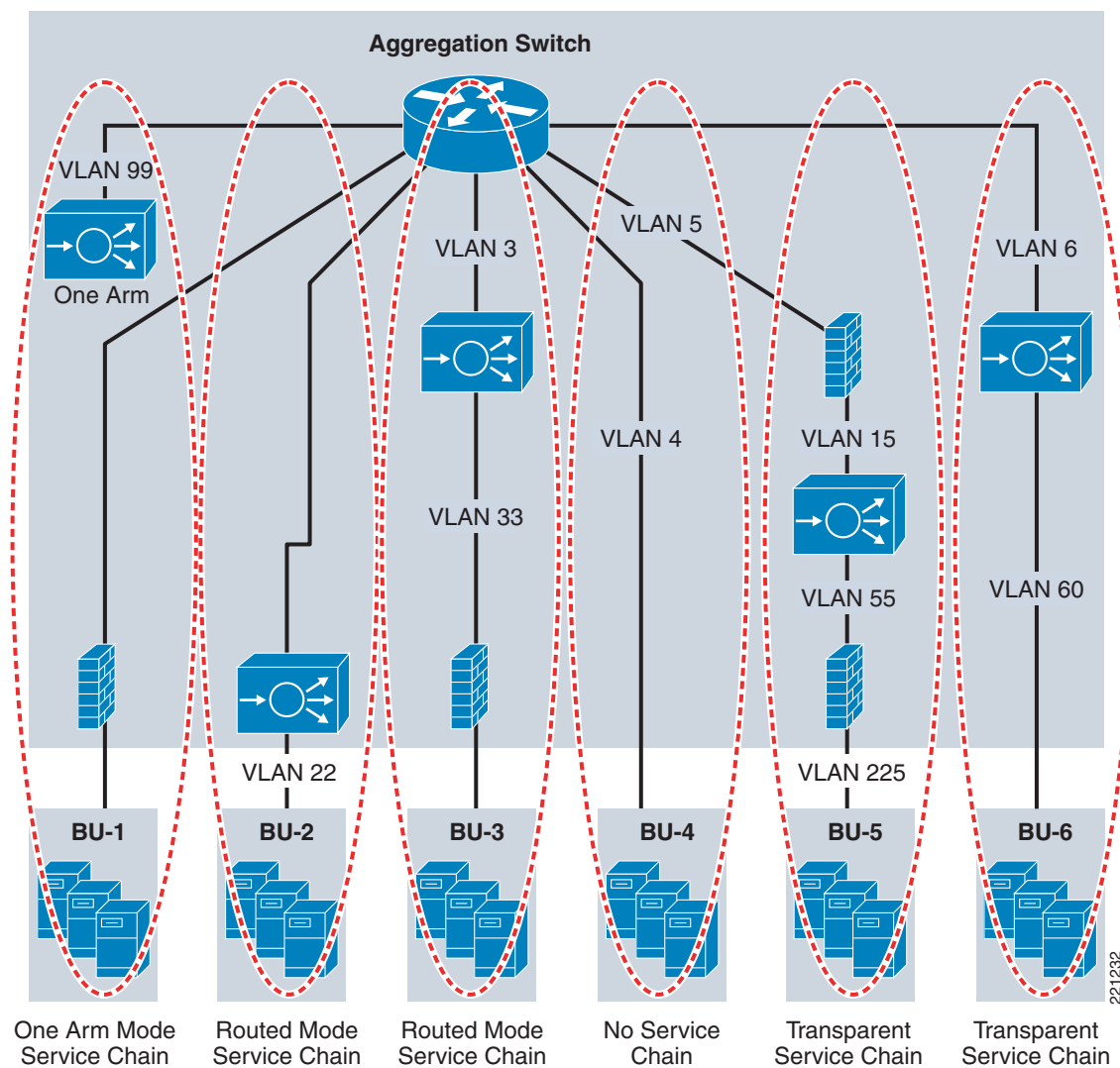
ACE Virtualization

Virtualization is a prevalent trend in the enterprise today. From virtual application containers to virtual machines, the ability to optimize the use of physical resources and provide logical isolation is gaining momentum. The advancement of virtualization technologies includes the enterprise network and the intelligent services it offers.

The ACE supports device partitioning where a single physical device may provide multiple logical devices. This virtualization functionality allows system administrators to assign a single virtual ACE device to a business unit or application to achieve application performance goals or service-level agreements (SLAs). The flexibility of virtualization allows the system administrator to deploy network-based services according to the individual business requirements of the customer and technical requirements of the application. Service isolation is achieved without purchasing another dedicated appliance that consumes more space and power in the data center.

Figure 9 shows the use of virtualized network services afforded via the ACE and Cisco Firewall Services Module (FWSM). In this diagram, a Catalyst 6500 housing a single ACE and FWSM supports the business processes of five independent business units. The system administrator determines the requirements of the application and assigns the appropriate network services as virtual contexts. Each context contains its own set of policies, interfaces, resources, and administrators. The ACE and FWSMs allow routed, one-arm, and transparent contexts to co-exist on a single physical platform.

Figure 9 Service Chaining via Virtualized Network Services



Note

For more information on ACE virtualization, see the *Application Control Engine Module Virtualization Configuration Guide* at the following URL:

http://www.cisco.com/en/US/products/hw/modules/ps2706/products_configuration_guide_book09186a00806882c6.html

TCP Reuse

TCP reuse allows the ACE to recycle TCP connections to the server farm, essentially reducing the load on the application servers. Servers use RAM to open and maintain connections to clients. RAM is a finite resource that directly impacts server performance. The ACE module allows persistent TCP connections to the application server and reclaims them for use by multiple clients.

**Note**

It is important to verify that the MSS and TCP options on the server and ACE are identical. For logging consistency, use HTTP header insertion to maintain the source IP address of clients when TCP reuse is in use.

HTTP Header Insertion

The ACE HTTP header insertion feature allows a system administrator to insert a generic string value or to capture the following request specific values:

- Source IP address
- Destination IP address
- Source port
- Destination port

HTTP header insertion is especially useful when TCP reuse or the source address of the request may be determined via NAT. HTTP header insertion allows service logs to reflect the original source IP address of the request. [Figure 10](#) shows the insertion of an HTTP header under the name “X-forwarder”, reflecting the source IP address of the request.

Figure 10 *HTTP Header Insertion Example*

```
GET / HTTP/1.1
X-forwarder: 192.168.30.11
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: oraclelll.eselab.com
Connection: Keep-Alive
Cookie: oracle.uix=0^GMT-4:00; ACEOptimized=R3691042226
```

22/233

Session Persistence

Session persistence is the ability to forward client requests to the same server for the duration of a session. Oracle recommends HTTP session persistence for their E-Business Suite environment via the following:

- IP sticky
- Cookie sticky

ACE supports each of these methods, but given the presence of proxy services in the enterprise, Cisco recommends using the cookie sticky method to guarantee load distribution across the server farm.

[Figure 10](#) shows the “ACEOptimized” cookie inserted into the client E-Business request.

In addition, ACE supports the replication of sticky information between devices and their respective virtual contexts. This provides a highly available solution that maintains the integrity of each session.

MAC Sticky

The ACE is capable of reverse path forwarding (RPF) based on the source MAC address on a VLAN interface of the request. This feature allows for transparency at Layer 3 and provides deterministic traffic flows at Layer 2 through the ACE. Cisco Wide Area Application Services (WAAS) devices deployed as a server farm under the ACE take advantage of this feature, guaranteeing that the same WAE device consistently manages each TCP session.

**Note**

This feature is not compatible with Layer 3 (IP)-based RPF.

Transparent Interception

Load balancers typically perform a NAT function to conceal the real server IP addresses residing in the retail data center, which means that the virtual IP address (VIP) is transformed and the request is forwarded to a real server. In addition to supporting this functionality, the ACE allows the system administrator to disable NAT for particular server farms, which is a desirable behavior for both firewall load balancing deployments and WAAS server farms.

**Note**

Transparent interception allows the WAE devices to perform their application optimization functionality without changing the Layer 3 information of the session.

Allowed Server Connections

Retail data centers typically perform due diligence on all deployed server and network devices, determining the performance capabilities to create a more deterministic, robust, and scalable application environment. The ACE allows the system administrator to establish the maximum number of active connections values on a per-server basis and/or globally to the server farm. This functionality protects the end device, whether it is an application server or network application optimization device such as the WAE.

Route Health Injection

Route health injection (RHI) allows the ACE to advertise host routes to any number of virtual IP addresses hosted by the device. The injection of the host route to the remaining network offers Layer 3 availability and convergence capabilities to the application environment.

Health Monitoring

The ACE device is capable of tracking the state of a server and determining its eligibility for processing connections in the server farm. The ACE uses a simple pass/fail verdict but has many recovery and failures configurations, including probe intervals, timeouts, and expected results. Each of these features contributes to an intelligent load balancing decision by the ACE context.

Following are the predefined probe types currently available on the ACE module:

- ICMP
- TCP
- UDP
- Echo (TCP/UDP)
- Finger
- HTTP
- HTTPS
- FTP
- Telnet
- DNS

- SMTP
- IMAP
- POP
- RADIUS
- Scripted (TCL support)

Note that the potential probe possibilities available via scripting make the ACE an even more flexible and powerful application-aware device. In terms of scalability, the ACE module can support 1000 open probe sockets simultaneously.

**Note**

In the E-Business suite environment, the HTTP probe verified the state of the entire application stack by requesting a page requiring APPL_TOP and database services.

Firewall Services Module

Overview

The Cisco Firewall Services Module (FWSM) is a stateful packet inspection engine that delivers access control security between network segments. The FWSM is an integrated service module available on the Catalyst 6500 platform that supports the following two modes of operation:

- Routed mode—The FWSM is considered a next hop in the network.
- Transparent mode—The FWSM bridges traffic between VLAN segments.

FWSM Virtualization

The FWSM supports device partitioning, allowing a single FWSM to be virtualized into multiple security contexts. The security contexts are logically isolated using independent security rules and routing tables. The system administrator can define up to 100 security contexts on a single FWSM. In addition, security context deployments support either routed or transparent mode. [Figure 9](#) shows several configuration options available with the security contexts of the FWSM. FWSM security contexts provide a flexible, scalable solution for data center application deployments.

**Note**

The Oracle E-Business suite application environment set up for this test document used security contexts in front of the APPL_TOP and database servers. For more information on leveraging the capabilities of the ACE and FWSM technologies in Oracle E-Business suite environments, see *Integrating Oracle E-Business Suite 11i in the Cisco Data Center* at the following URL:
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns50/c649/ccmigration_09186a00807688ce.pdf

Wide Area Application Engine

To appreciate how WAAS provides WAN and application optimization benefits to the enterprise, consider the basic types of centralized application messages that are transmitted between stores. For simplicity, two basic types are identified:

- Bulk transfer applications—Transfer of files and objects, such as FTP, HTTP, and IMAP. In these applications, the number of roundtrip messages may be few, and may have large payloads with each packet. Examples include web portal or thin client versions of Oracle, SAP, Microsoft (SharePoint, OWA) applications, e-mail applications (Microsoft Exchange, Lotus Notes), and other popular business applications.
- Transactional applications—High number of messages transmitted between endpoints. Chatty applications with many roundtrips of application protocol messages that may or may not have small payloads. Examples include Microsoft Office applications (Word, Excel, PowerPoint, and Project).

WAAS uses the technologies described in the following subsections to provide a number of features, including application acceleration, file caching, print service, and DHCP to benefit both types of applications.

Advanced Compression using DRE and Lempel-Ziv Compression

Data Redundancy Elimination (DRE) is an advanced form of network compression that allows Cisco WAAS to maintain an application-independent history of previously-seen data from TCP byte streams. Lempel-Ziv (LZ) compression uses a standard compression algorithm for lossless storage. The combination of using DRE and LZ reduces the number of redundant packets that traverse the WAN, thereby conserving WAN bandwidth, improving application transaction performance, and significantly reducing the time for repeated bulk transfers of the same application.

Transport File Optimizations

Cisco WAAS Transport File Optimizations (TFO) employs a robust TCP proxy to safely optimize TCP at the WAE device by applying TCP-compliant optimizations to shield the clients and servers from poor TCP behavior because of WAN conditions. Cisco WAAS TFO improves throughput and reliability for clients and servers in WAN environments through increases in the TCP window sizing and scaling enhancements as well as implementing congestion management and recovery techniques to ensure that the maximum throughput is restored if there is packet loss.

Common Internet File System Caching Services

Common Internet File System (CIFS), used by Microsoft applications, is inherently a highly chatty transactional application protocol where it is not uncommon to find several hundred transaction messages traversing the WAN just to open a remote file. WAAS provides a CIFS adapter that can inspect and to some extent predict what follow-up CIFS messages are expected. By doing this, the local WAE caches these messages and sends them locally, significantly reducing the number of CIFS messages traversing the WAN.

Print Services

WAAS provides native SMB-based Microsoft print servers locally on the WAE device. Along with CIFS optimizations, this allows for store server consolidation at the data center. Having full-featured local print services means less traffic transiting the WAN. Without WAAS print services, print jobs are sent from a store client to the centralized server(s) across the WAN, then back to the store printer(s), thus transiting the WAN twice for a single job. WAAS eliminates the need for either WAN trip.



Note

For more information on these enhanced services, see the *Cisco Wide Area Application Services (WAAS) V4.0 Technical Overview* at the following URL:

http://www.cisco.com/en/US/products/ps6870/products_white_paper0900aecd8051d5b2.shtml

Design and Implementation Details

Design Goals

The retail enterprise network is a platform constructed to support a myriad of business functions; more specifically, applications. The traditional perception of the network relegates its role to one of data transport, providing a reliable fabric for the enterprise. This is a fundamental responsibility of the network infrastructure and should be enhanced rather than neglected. In addition to transport, the ubiquitous nature of the enterprise network fabric allows the introduction of intelligent network services to support business applications. This evolution of the network as an enterprise service platform is natural and supports the following Oracle application objectives:

- High availability
- Scalability
- Security
- Optimization
- Manageability

The Cisco Lean Retail data center architecture is a holistic approach that allows the network and the applications it supports to work together. The primary goals of this design are to increase the performance, availability, scalability, and manageability of enterprise applications in the data center, while simultaneously providing a secure environment. In addition, this design reduces the complexity and implementation time of enterprise applications in the data center using virtualization technologies and network design best practices. The remainder of this document focuses on each of these objectives when deploying an Oracle E-Business Suite 11i application using the services of the Cisco Lean Retail data center infrastructure and Intelligent Retail Network store solutions.

Design Implementation

This section focuses on the use of the Cisco Wide Area Application Engine (WAE) in conjunction with the Cisco Application Control Engine (ACE) and Cisco Firewall Services Module (FWSM) in the retail data center. The data center deployment described has the ACE in a routed mode with the FWSM deployed transparently. WAE service devices deployed in the data center benefit from the availability and scalability services of the ACE platform.

These designs specifically address a multi-tier deployment of the Oracle E-Business Suite application in the Cisco data center infrastructure architecture. The designs provide centralized load balancing, security, and optimization services for the application. In addition, the virtualization capabilities of both the FWSM and the ACE allow a single physical device to provide multiple logical devices to support a variety of application environments. System administrators can assign a single virtual device to a business unit or application to achieve application performance goals, requirements, or service-level agreements. (See [Figure 9](#)).

Store Designs

The WAAS solution requires a minimum of two WAE devices to auto-discover and deliver applicable application optimizations. To leverage these transparent optimizations across the WAN, deploy one or more WAEs at the store and one or more WAEs at the retail data center, depending on availability and scalability requirements.

Within the existing store topologies, the WAE devices may be positioned in one of the following models:

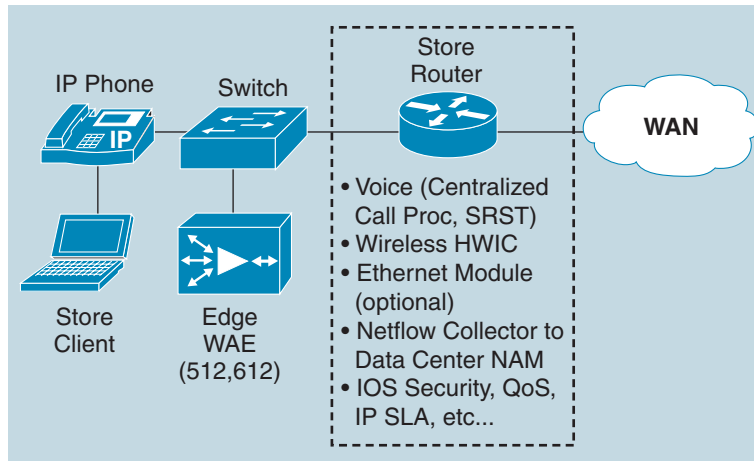
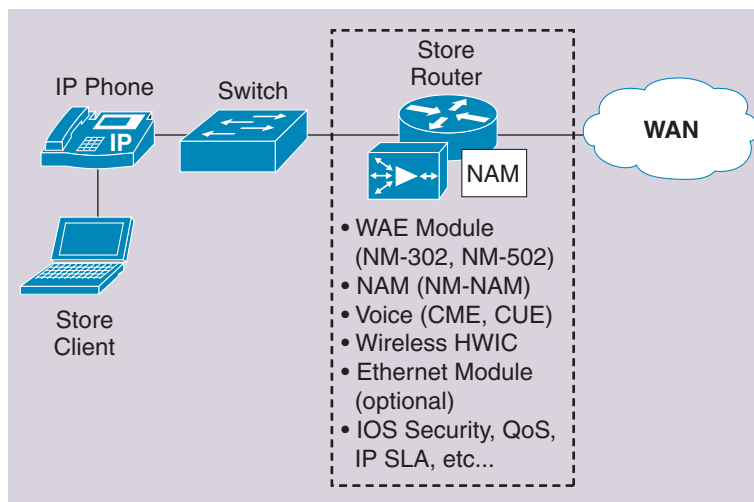
- Extended store
- Consolidated store

Figure 11 shows each of these design models. WAE Store Deployment Models shows each of these design models. The extended services store offloads the WAE device from the local store router and leverages the available ports on a local switch. The consolidated store model uses an integrated services router, providing a comprehensive solution within a single platform. Each of these models provides application optimization services. The retailer must consider the scalability and availability requirements of each store for WAAS and other network services before choosing a deployment model.

**Note**

The testing performed to create this document used each of these design models. For more information on Cisco WAE store deployments, see *Enterprise Branch Wide Area Application Services Design Guide* at the following URL:

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns477/c649/ccmigration_09186a008081c7d5.pdf

Figure 11 WAE Store Deployment Models**Store 1**
Extended Services Store**Store 2**
Consolidated Store

WAAS technology requires the efficient and predictable interception of application traffic to produce results. It is critical that the WAE device see the entire TCP conversation. At the WAN edge, Cisco routers support the following four methods of traffic interception:

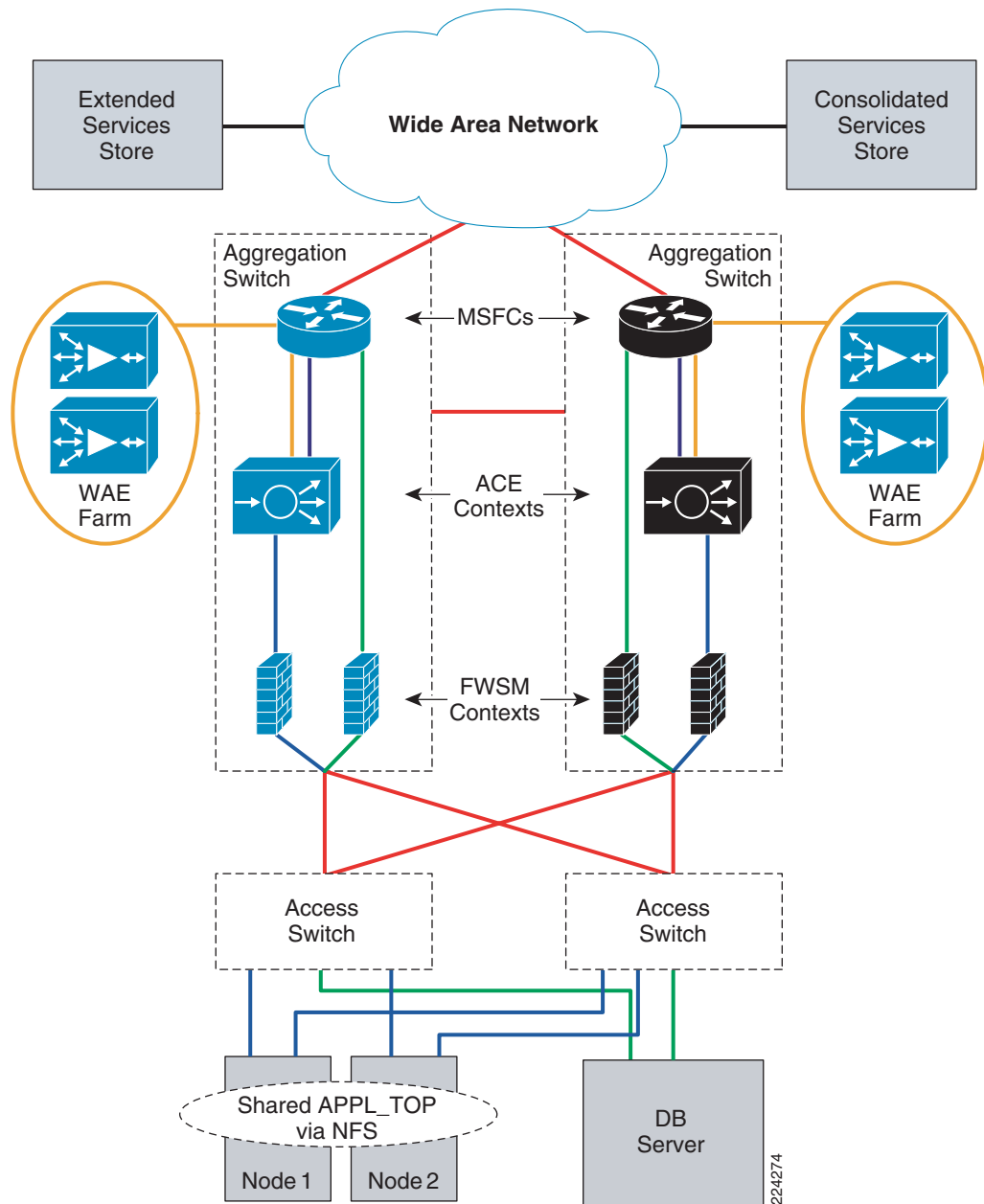
- Policy-based routing (PBR)
- Web Cache Communications Protocol (WCCP) v2
- Service policy with ACE
- Inline hardware

WCCPv2 is the most common method used in the store environment; therefore, WCCPv2 has been leveraged for this documentation.

ACE Routed Mode Design

[Figure 12](#) details the data center networking topology used in the test Oracle application environment. Each of the test stores, extended or consolidated, connect to the data center across the WAN and leverage the services of the enterprise edge and data center core (not pictured here) that attach to the aggregation layer of the data center.

Best practices for the Cisco data center infrastructure offer predictable Layer 2 and Layer 3 traffic patterns, permitting the efficient application of network services. From a Layer 2 perspective, the data center must be scalable, flexible, and robust. Given current application clustering, network interface card (NIC) teaming, and virtual machine requirements, the presence of a Layer 2 redundancy protocol is required and will be for the foreseeable future. At this time, Cisco recommends the use of Rapid Per VLAN Spanning Tree (RPVST)+ to achieve sub-second Layer 2 convergences and deterministic flows in the data center.

Figure 12 Logical Topology using ACE in Routed Mode

The Layer 3 devices in the aggregation layer use a redundancy protocol such as Hot Standby Routing Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP) to create a robust IP network. The Multilayer Switch Feature Card (MSFC) employs an Interior Gateway Protocol (IGP), for instance OSPF or EIGRP, to distribute route information to the external network, including updates relative to the state of the E-Business Suite applications. This information is derived from the RHI messages received from the active ACE context. In addition to Layer 2 and Layer 3 functionality, the data center aggregation switches are a natural convergence area in the network, and therefore an ideal location to apply intelligent network services.

**Note**

For more information on data center infrastructure design best practices, see the following URL:
<http://www.cisco.com/go/srnd/datacenter>.

The ACE virtual context in this design is in routed mode, meaning that the default gateway of the APPL_TOP servers points to an alias IP address existing on the virtual ACE context. This alias IP is shared across the two virtual ACE contexts, offering a redundant L3 topology for the server farms. To transparently introduce the application optimization services afforded via WAE appliances, it is necessary to leverage the routing capabilities of an ACE context. Remember that WAE appliances do not alter the IP information on the packet. The IP source and destination information remains unchanged. Therefore, it is necessary to use dedicated VLANs in and out of the ACE context to control the logical flow of traffic into the ACE, to the WAE farm, and egress from the ACE to the server. Essentially, VLANs segmentation prevents the “looping” of TCP flows. Defining an “inbound” client-facing VLAN, a dedicated WAE VLAN, and an “outbound” server-facing VLAN from the ACE perspective effectively avoids this issue by providing predictable traffic patterns between all the parties involved.

The ACE virtual context determines the state of the Oracle environment via health probes. Using this information, the ACE context manages the workload for each Oracle server and the state of the VIP, making the environment highly available and scalable by potentially supporting thousands of E-Business servers. The ACE module currently supports the following load balancing algorithms:

- Round-robin
- Least connections
- Hash address
- Hash cookie
- Hash header
- Hash URL

The ACE allows the system administrator to define a “server farm” of WAE devices to provide application optimization services in the data center. The WAE appliances benefit from the same health monitoring and scalability services provided via the ACE. The system administrator may then balance the E-Business suite workload across many Oracle application servers and numerous WAE devices front ending the Oracle application environment.

The ACE context enforces session persistence to the APPL_TOP servers via IP or Cookie based sticky methods. The WAE devices that reside transparently in the traffic flow leverage Layer2 MAC based sticky to guarantee efficient traffic patterns between the APPL_TOP servers and remote clients.

In [Figure 12](#), multiple FWSM contexts provide security services to the Oracle APPL_TOP and database tiers. The segmented traffic patterns between tiers in the multi-tier Cisco data center infrastructure allows for granular security policies, as well as application services, to be applied at each layer of the stack. In this instance, there are two transparent firewall contexts deployed. Transparent firewalls are “bumps in the wire”, bridging traffic between VLAN segments. Transparent firewalls allow the construction advanced Layer 2 topologies by passing Bridge Protocol Data Units (BPDUs) between VLAN segments.

Traffic Pattern Overview

This section describes the traffic pattern flows in and out of the data center when deploying the WAAS, ACE, and FWSM devices. The following connections are discussed:

- Client-to-server
- Server-to-server

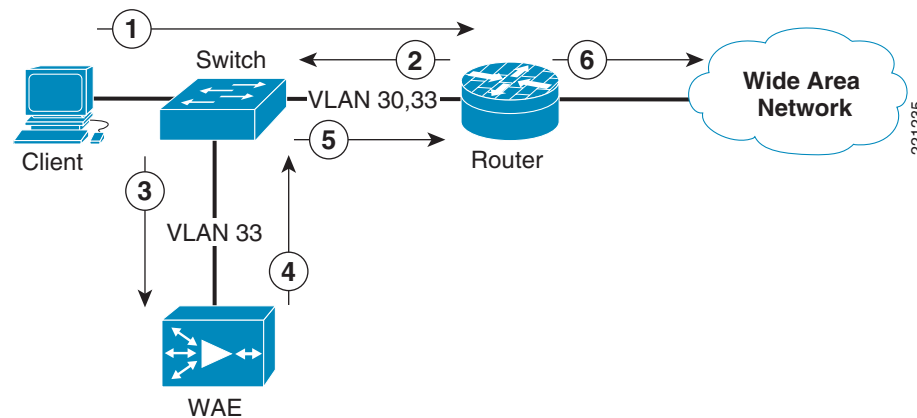
Client-to-Server Traffic Flow

Figure 13 through Figure 16 detail the traffic flow from a store user connecting to the E-Business suite application residing in the data center. The application is accessible to the store user across the WAN. The store and data center employ WAAS application optimization services. This example uses an extended services store configuration; however, the use of an ISR in a consolidated store configuration would yield exactly the same traffic patterns from a data center perspective.

The successful optimization of an E-Business suite transaction across the WAN and data center includes the following steps:

1. The store client initiates a connection to the Oracle E-Business suite environment via the ACE VIP on the service module. TCP SYN sent to the VIP.

Figure 13 Traffic Pattern—Extended Service Store Example



2. The store router transparently intercepts the TCP SYN using WCCPv2. WCCPv2 makes a load balancing decision and the router L2 redirects the flow to a specific WAE device in the service group.



Note

Leverage WCCPv2 ACLs to only redirect traffic destined for the WAN. Traffic confined to the store LAN would not benefit from WAE services and would simply introduce more load to the local WAE store devices.

3. The store switch forwards the packet to the WAE device.
4. The WAE device applies a new TCP option (0x21) to the packet if the application is identified for optimization by an application classifier. The WAE adds its device ID and application policy support to the new TCP option field. This option is examined and understood by other WAEs in the path as the ID and policy fields of the initial WAE device. The initial ID and policy fields are not altered by another WAE. Figure 14 captures the WAE TCP option added to a client SYN in the test bed.

Figure 14 **WAE TCP Option Trace**

```

Packet Number: 884 - Time: Apr 25, 2007 13:35:32.643 - Packet Length: 78 bytes - Capture Length: 78 bytes
+ ETH Ethernet II, Src: 00:0b:fc:fe:1b:03 (00:0b:fc:fe:1b:03), Dst: 00:14:5e:a4:67:04 (00:14:5e:a4:67:04)
+ VLAN 802.1Q Virtual LAN
+ IP Internet Protocol, Src: 192.168.30.11 (192.168.30.11), Dst: 10.20.100.100 (10.20.100.100)
- TCP Transmission Control Protocol, Src Port: 32252 (32252), Dst Port: 80 (80), Seq: 877759286, Ack: 0, Len: 0
  TCP Source port: 32252 (32252)
  TCP Destination port: 80 (80)
  TCP Sequence number: 877759286
  TCP Header length: 40 bytes
  TCP Flags: 0x0002 (SYN)
  TCP 0... .. = Congestion Window Reduced (CWR): Not set
  TCP ..0.. .. = ECN-Echo: Not set
  TCP ...0.. .. = Urgent: Not set
  TCP ...0.. .. = Acknowledgment: Not set
  TCP ....0... = Push: Not set
  TCP ....0... = Reset: Not set
  TCP ....1.. = Syn: Set
  TCP ....0.. = Fin: Not set
  TCP Window size: 65535
  TCP Checksum: 0xb5eb [correct]
  TCP Options: (20 bytes)
  TCP Maximum segment size: 1432 bytes
  TCP NOP
  TCP NOP
  TCP SACK permitted
  TCP Unknown (0x21) (12 bytes)

```

221236

Figure 15 is a screenshot defining the HTTP applications recognized by the WAEs in the test bed.

Figure 15 **Central Manager Application Classifier Example**

System Status | Devices: 1 Device, Critical | Home | Help | Logout

Devices | Device Groups | Locations

Expand All | Hide Advanced | Modifying Application Classifier, HTTP for WAE, DC02-WAE7326-2...

Contents

- Home
- Activation
- File Services
- Acceleration
 - Enabled Features
 - Acceleration TCP Settings
- Policies
 - Definitions
 - Prioritization
 - Statistics
- Topology
- Print Services
- General Settings
- Interception
- Monitoring
- Assign Groups

Application Classifier

Name: HTTP

Comments: HTTP based applications in the data center.

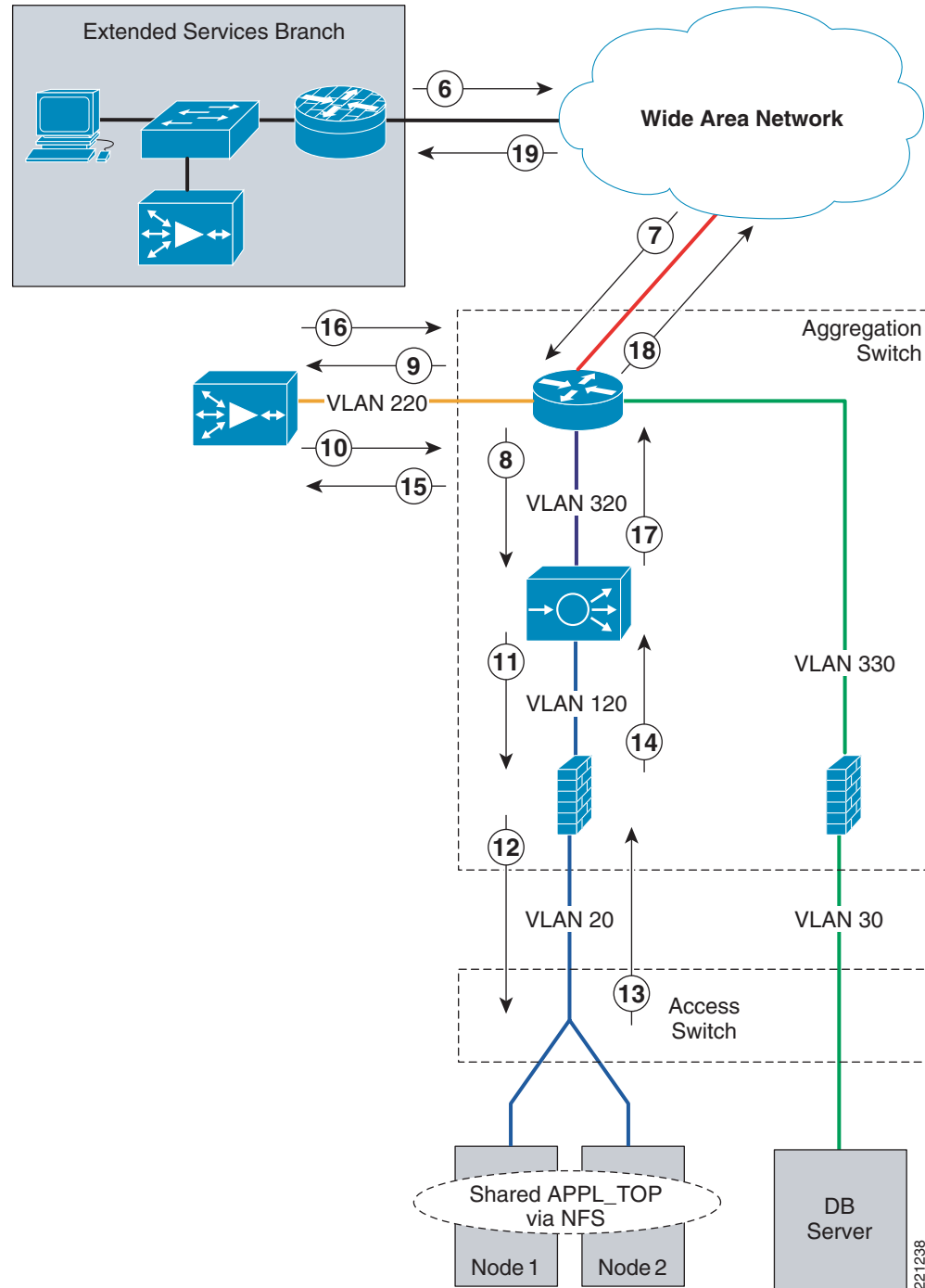
Configure Match Conditions

Match All	Source IP Address	Source IP Wildcard	Source Port	Destination IP Address	Destination IP Wildcard	Destination Port
No						80
No						8080
No						8000
No						8001
No						3128

221237

- The store switch forwards the packet to the store router that is configured as the default gateway for the WAE devices. Note that the source and destination IP addresses of the initial request of the remote client remain unchanged.
- The router forwards the packet to the VIP address across the WAN.
- As shown in Figure 16, the SYN has traversed the WAN and data center core and is entering the root aggregation switch in the data center.

Figure 16 Traffic Pattern—ACE-WAE Data Center Deployment Example



8. The MSFC forwards the packet to the VIP address advertised by the active ACE context via RHI to the network.
9. The service policy located on the public or outside interface of the ACE context directs traffic destined for the E-Business suite environment to the WAE farm. The following sample configuration shows this behavior defined as ORACLE_TCP_TRAFFIC.

The configuration states that all traffic destined to the ORACLE_VIP should be load balanced and redirected to the real servers defined under the WAE-SERVERS server farm. The ACE context does not alter the IP source or destination address but transparently load balances the traffic; the *transparent* keyword indicates that no network address translation (NAT) will occur.

```
serverfarm host WAE-SERVERS
transparent
probe WAE
rserver DC01-ESE-WCE2
inservice
rserver DC01-ESE-WCE3
inservice
rserver DC02-WAE7326-2
inservice
!
class-map match-all ORACLE_VIP
  2 match virtual-address 10.20.100.100 tcp eq www
!
policy-map type loadbalance first-match WAE_TRAFFIC
class class-default
serverfarm WAE-SERVERS
!
policy-map multi-match ORACLE_TCP_TRAFFIC
class ORACLE_VIP
loadbalance vip inservice
loadbalance policy WAE_TRAFFIC
loadbalance vip icmp-reply
!
interface vlan 320
description client VLAN
ip address 10.80.1.4 255.255.0.0
ip options allow
alias 10.80.1.6 255.255.0.0
peer ip address 10.80.1.5 255.255.0.0
no normalization
no icmp-guard
service-policy input ORACLE_TCP_TRAFFIC
no shutdown
```

The ACE context has access control and HTTP deep packet inspection capabilities. HTTP deep packet inspection allows the system administrator to monitor the HTTP protocol, permitting or denying traffic based on user-defined traffic policies. The security features covered by HTTP application inspection include the following:

- RFC compliance monitoring and RFC method filtering (RFC 2616)
- Content, URL, and HTTP header length checks
- Transfer-encoding methods
- Content type verification and filtering
- Port 80 misuse

Using the regular-expression capabilities of the ACE against HTTP data payloads allows for signature-based security decisions that are usually reserved for IDS/IPS devices.

10. The WAE device inspects the SYN packet and recognizes the presence of another WAE in the traffic flow; therefore, the WAE appends its ID and application policy support to the existing TCP option 0x21 field while storing the ID and application policy of the store WAE. The WAE forwards the packet to its default gateway, which is the alias IP address of the ACE. The following example shows

the configuration of the ACE interface to the WAE server farm VLAN. The WAE default gateway is the alias IP address (10.220.1.1) on this interface. In addition, this interface supports another service policy, `VIP_ORACLE_POLICY`, to load balance traffic to the `APPL_TOP` servers in the data center.

```
!
interface vlan 220
  description ** WAE Server Farm VLAN **
  ip address 10.220.1.2 255.255.0.0
  alias 10.220.1.1 255.255.0.0
  peer ip address 10.220.1.3 255.255.0.0
  no normalization
  mac-sticky enable
  no icmp-guard
  service-policy input VIP_ORACLE_POLICY
  no shutdown
  ip route inject vlan 320
```

11. The WAE VLAN interface employs the `VIP_ORACLE_POLICY` to all input traffic on the interface. The policy, as shown in the following configuration, forwards traffic destined to the Oracle E-Business suite VIP to the real servers defined in the `APPL_TOP_FARM` server farm. The `APPL_TOP_FARM` servers leverage cookie-based sticky to provide session persistence and TCP reuse functionality in this configuration example.

```
!
serverfarm host APPL_TOP_FARM
  description This is the APPL_TOP server farm.
  probe HTTP_PROBE
  rserver OracleNode1 8000
    inservice
  rserver OracleNode2 8000
    inservice
!
sticky http-cookie ACEOptimized sticky-ace-cookie
  cookie insert
  replicate sticky
  serverfarm APPL_TOP_FARM
!
policy-map type loadbalance first-match ORACLE_POLICY
  class class-default
    sticky-serverfarm sticky-ace-cookie
!
policy-map multi-match VIP_ORACLE_POLICY
  class ORACLE_VIP
    loadbalance vip inservice
    loadbalance policy ORACLE_POLICY
    loadbalance vip icmp-reply
    appl-parameter http advanced-options TCP-reuse
```

The ACE context forwards the flow to the real `APPL_TOP` servers that are protected by a transparent firewall context. At this stage, the destination IP address of the flow has been translated from the VIP to an IP address of a real `APPL_TOP` server.



Note

The TCP option 0x21 is no longer present on the SYN packet forwarded to the “outside” interface of the FWSM virtual context. The ACE module strips this option and forwards the packet as dictated by its default behavior. For more information, see the latest Application Control Engine Module Security Configuration Guide at the following URL:
http://www.cisco.com/en/US/products/hw/modules/ps2706/products_installation_and_configuration_guides_list.html.

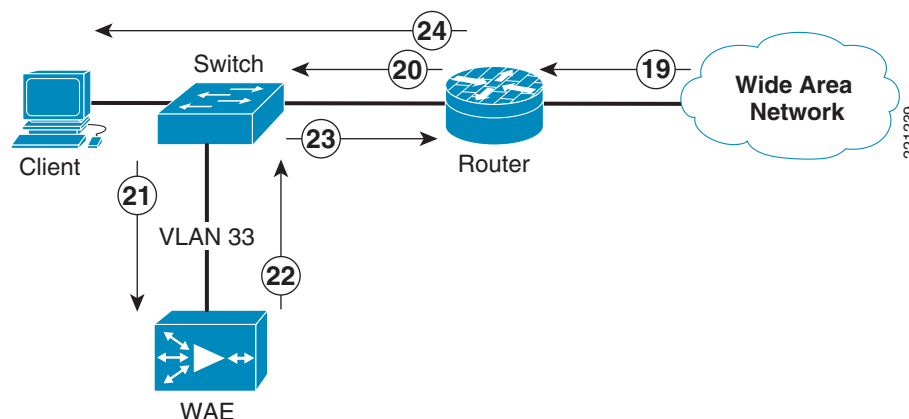
12. The FWSM virtual context bridges permitted traffic from the “outside” to “inside” interface of the firewall context to access the Oracle 11i environment.
13. The APPL_TOP server responds with a SYN/ACK to the client SYN.
14. The FWSM bridges the traffic to the ACE module.
15. The ACE context performs reverse NAT on the SYN/ACK response from the APPL_TOP server and forwards the packet back to the WAE, leveraging the MAC-sticky feature. Step 10 shows the sample interface configuration with MAC-sticky.



Note The MAC-sticky feature ensures that the TCP flow returns to the WAE that originally processed the incoming SYN. This ensures a consistent auto-discovery process by the WAE devices.

16. The WAE receives the SYN/ACK and adds TCP option 0x21 to the packet with its ID and application policy support. The SYN/ACK is then forwarded to its default gateway, the ACE interface.
17. The ACE directs the packet to the client via its default gateway, the MSFC.
18. The MSFC routes the packet to the client by way of the WAN.
19. The remote extended service store router receives the SYN/ACK from the APPL_TOP server front ended by the ACE VIP. The destination address is the client IP address, and the source IP address is the ACE VIP.
20. The router redirects the input traffic to the WAE using an implementation of WCCPv2 using a Layer 2 redirection. (See [Figure 17.](#))

Figure 17 Traffic Pattern—Extended Service Store Return Flow Example



21. The switch forwards the packet to the WAE appliance.
22. The WAE device is aware of the WAE in the data center because the SYN/ACK TCP option 0x21 contains an ID and application policy. The auto-negotiation of the policy occurs as the store WAE compares its application-specific policy to that of its remote peer defined in the TCP option. At this point, the data center WAE and store WAE have determined the application optimizations to apply on this specific TCP flow.

The **show tfo connection** command on the store WAE details the results of auto-negotiation for each TCP flow. Following is a portion of the output showing the policy negotiation between the client and Oracle VIP:

```
Connection Id: 323
```

```

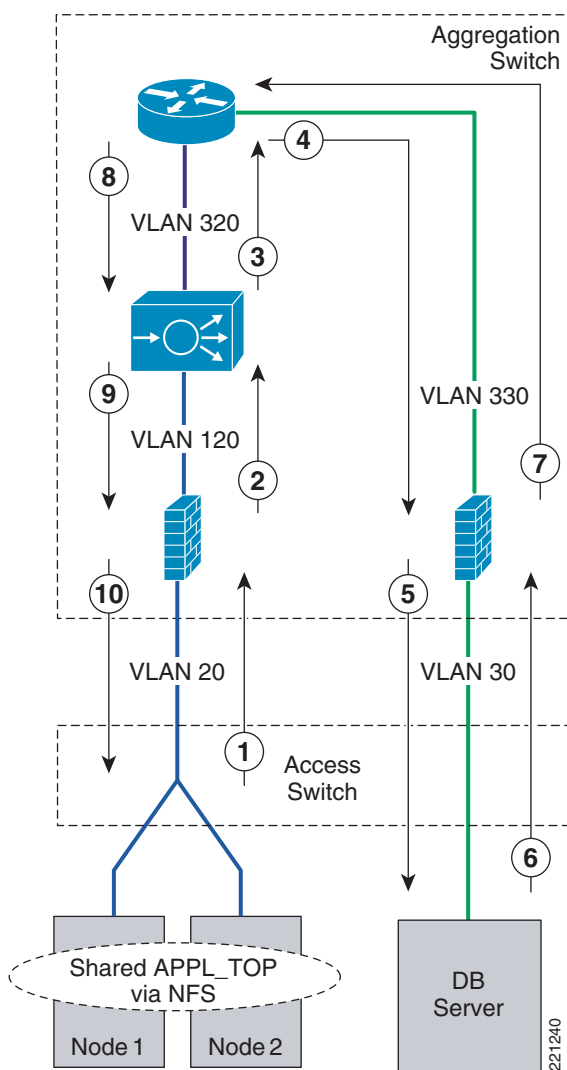
Start time:           Mon May  7 08:10:22 2007
Peer Id:              00:14:5e:95:d1:3d
Connection type:      Ext. Server
Source IP Address:    192.168.30.11
Source Port Number:   11773
Destination IP Address: 10.20.100.100
Destination Port Number: 80
Our policy:           TCP_OPTIMIZE + DRE + LZ
Peer policy:          TCP_OPTIMIZE + DRE + LZ
Negotiated policy:    TCP_OPTIMIZE + DRE + LZ
Applied policy:       TCP_OPTIMIZE + DRE + LZ

```

23. The SYN/ACK packet is forwarded to the store router, which is the default gateway for the WAE.
24. The router directs the SYN/ACK response to the client.

Server-to-Database Traffic Flow

Figure 18 shows the traffic pattern between the APPL_TOP servers and the Oracle database server when using an ACE virtual context in routed mode and leveraging the FWSM virtual context in transparent mode.

Figure 18 *APPL_TOP Server to Database Server Traffic Pattern*

The APPL_TOP servers initiate the TNS connection with the database server. The ACE module configuration allows this data traffic to pass through via ACLs without performing any load balancing services. In addition to access control, the firewall context provides stateful packet inspection services.

**Note**

Traffic between the APPL_TOP and database servers is not processed by the WAE farm because only traffic destined to the public VIP on the ACE is transparently redirected to the WAE devices.

The following steps take place:

1. The APPL_TOP server initiates a database request via a TCP connection. The request is directed to its default gateway on the ACE. The destination IP address is that of the database server and the destination port is 1521, the well-known TNS port.
2. The application tier firewall context receives the request on its inside interface. The FWSM context bridges the traffic to the ACE virtual context. The firewall virtual context creates a valid connection entry in its local connection table.

3. The ACE context routes the TNS request to the MSFC. The MSFC is the default gateway for the ACE context.
4. The database tier firewall context receives the request on its outside interface. The FWSM context determines that TNS traffic is permitted and forwards the request to the database server, creating a new connection in its local connection table.
5. The firewall context forwards the TNS request to the database server.
6. The database server replies to the TNS request and forwards the response to its default gateway, the MSFC.
7. The firewall context bridges the traffic to the MSFC.
8. The MSFC routes the database server response to the APPL_TOP server via the ACE context.
9. The ACE context permits the returning database flow to pass through based on its access control lists and current connection entries.
10. The response is transparently bridged by the FWSM context to the originating server, based on the valid connection entry originally created by the initial TCP SYN packet. The TNS response reaches the APPL_TOP server.

Architecture Details

This section describes the application and network components of the test bed and includes the following sub-topics:

- Oracle E-Business Suite 11i Environment
- Oracle E-Business Suite 11i Environment with Integrated Network Services
- Additional Service Integration Options

Oracle E-Business Suite 11i Environment

This section details the application environment leveraged during testing, identifying the hardware and software components of the test bed.

Hardware

A single HP DL580 server supported the Oracle 11i database. Accessing this database server is a set of five HP DL580 servers housing the APPL_TOP nodes of this deployment. NFS services at the APPL_TOP layer allowed for a “shared” environment across the nodes. Each of the APPL_TOP HP DL580 servers are FiberChannel-attached to shared storage.

Software

Red Hat Enterprise Linux AS release 4 (Nahant Update 2) is the operating system used for all nodes in the test bed. The Oracle test environment consists of the following software packages:

- E-Business Suite 11i version 11.5.10.2
- Oracle Database version 9.2.06.0

Oracle E-Business Suite contains a sample database named Vision. The Vision database allows the generation of valid application traffic in the test bed using production-ready applications in the 11i suite.

A VMWare Virtual Infrastructure 3 environment, ESX 3.0, housed the Oracle EBS APPL_TOP nodes for testing. [Figure 19](#) is a virtual infrastructure snapshot showing the physical-to-virtual mapping of Node1 in the APPL_TOP environment. Node1 access shared storage across the SAN and currently resides on physical server 10.99.1.156. The virtual NIC (vNIC) of Node1 connects to a virtual machine port group named VM Network.

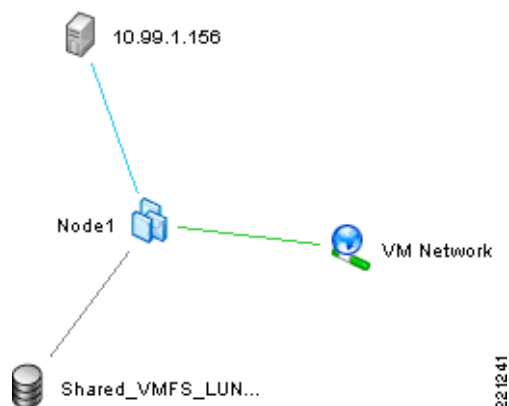
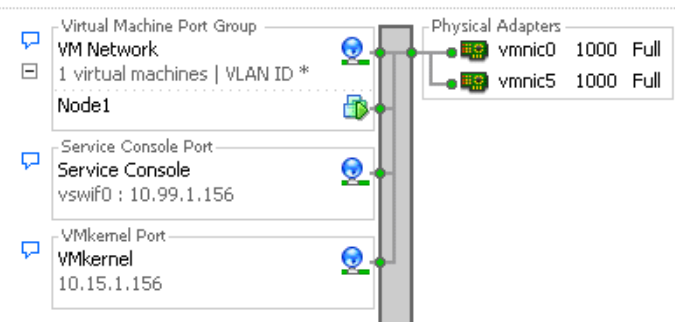
Figure 19 Sample Node Software Topology

Figure 20 shows the virtual switch configuration on each of the HP DL580 ESX servers. The virtual switch vSwitch0 has three “virtual” ports defined that map to distinct VLANs. In the example shown in Figure 20, the “VM Network” port group maps to VLAN 20, the APPL_TOP VLAN, and currently Oracle Node1 is leveraging its services.

Figure 20 Virtual Machine Network Connectivity**Networking**

Virtual Switch: vSwitch0

**Note**

For more information on the use of virtual machines in a Cisco data center, see *Integrating Virtual Machines into the Cisco Data Center Architecture* at the following URL: <http://www.cisco.com/go/srnd>.

Oracle E-Business Suite 11i Environment with Integrated Network Services

This section covers the introduction of network services into the Oracle E-Business Suite solution topology. Table 1 lists the network-related hardware and software components.

Table 1 Test Bed Network Components

Network Component	Hardware Model	Software Version
Aggregation/access switches	Catalyst 6500 w/Sup720	12.2(18)SXF5
Firewalls	WS-SVC-FWM-1	3.1(4)

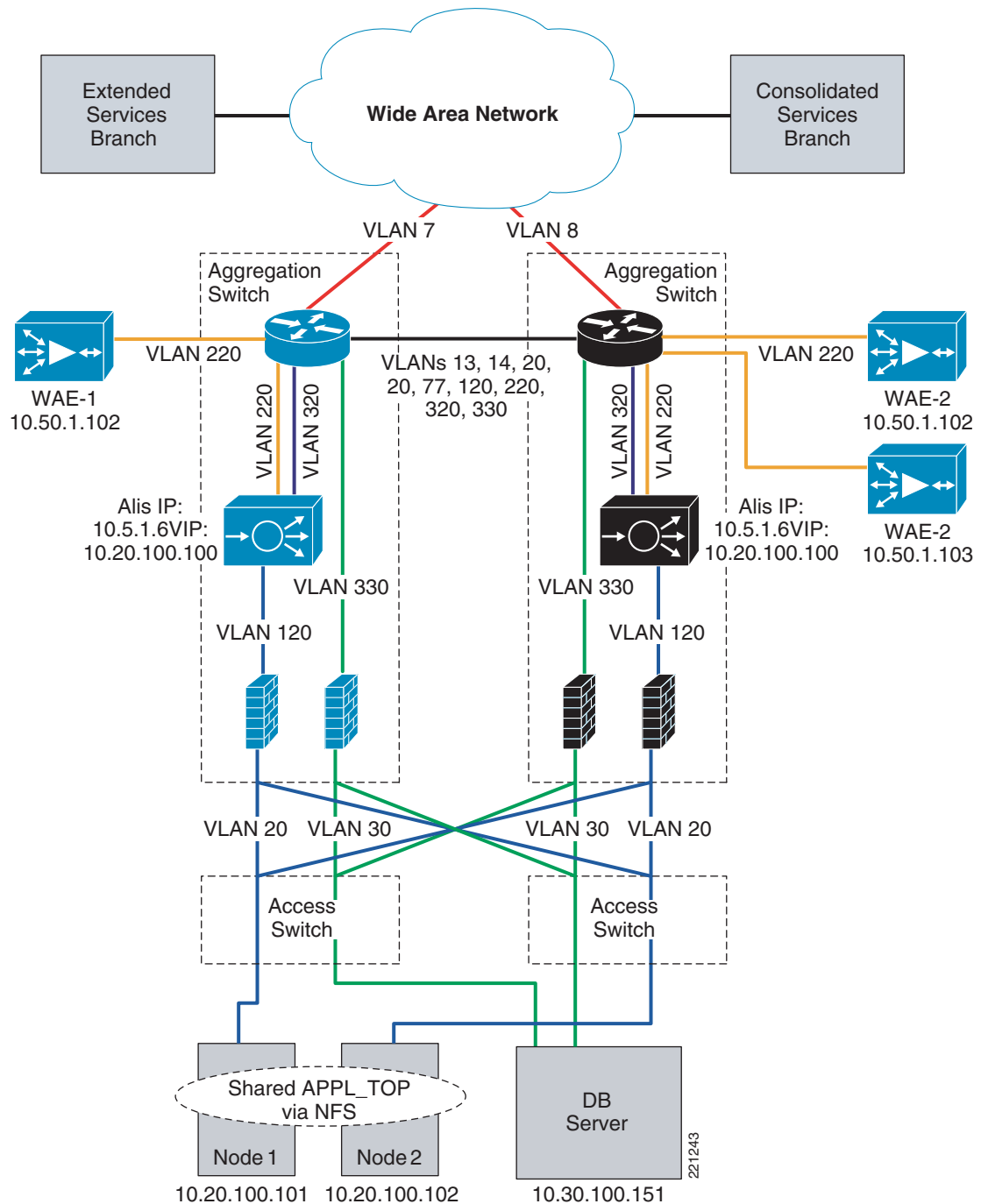
Table 1 **Test Bed Network Components (continued)**

Load balancer	ACE10-6500-K9	3.0(0)A1(4)
Wide Area Application Service	WAE-7326	4.0.7
SAN switches	MDS 9216i	SAN OS 3.0(3)

Topology

Figure 21 shows the Oracle E-Business Suite 11i application environment with the ACE virtual context in a routed mode design. The ACE context provides load balancing, session persistence, and security services to the application. In addition, the ACE context provides these services to a farm of WAE appliances that support application optimization technologies well-suited for E-Business suite deployments.

Figure 21



The routed mode design implies that the ACE is the default gateway for the APPL_TOP server farm. The gateway is accessible via the services of a transparent firewall context. The ACE and firewall context are deployed in an active/standby scenario with stateful failover. An independent pair of transparent virtual firewalls secures the database environment as well. The ability to segment and enforce granular traffic policies at each tier of the application topology is a powerful characteristic of this design.

At the foundation, the application leverages the high availability, scalability, and security features of the Cisco data center infrastructure at Layer 2 and Layer 3. The aggregation switch on the left in [Figure 21](#) represents the “root” of the spanning tree domain and the “active” HSRP Layer 3 interface. To provide efficient traffic patterns in the data center, Cisco recommends keeping active network service contexts aligned with the Layer 2 and 3 topologies. This prevents over utilization of ISLs that may support fault-tolerant protocols in addition to traffic relevant to the application.

The ISLs in the test bed are all 10 Gigabit Ethernet. The access layer switches are dual-homed to the aggregation switches and carry the APPL_TOP and database subnets. The servers are dual-homed to the access layer using an active/standby NIC teaming configuration.

Additional Integrated Service Options

This document addresses the integration of network services with the Oracle enterprise class application, E-Business Suite 11i. Server load balancing and security are fundamental services that may be leveraged by data center applications. In addition, this document details the integration of network-based application optimization services in the data center and store. However, these are not the only integrated network services available for the enterprise. The following network services are also accessible as service modules or appliances:

- SSL offloading (hardware-based option integrated into the ACE platform)
- Intrusion prevention systems (IPS)
- Intrusion detection systems (IDS)
- Network analysis devices
- Caching devices
- Alternative WAN optimization systems such as the Application Velocity System

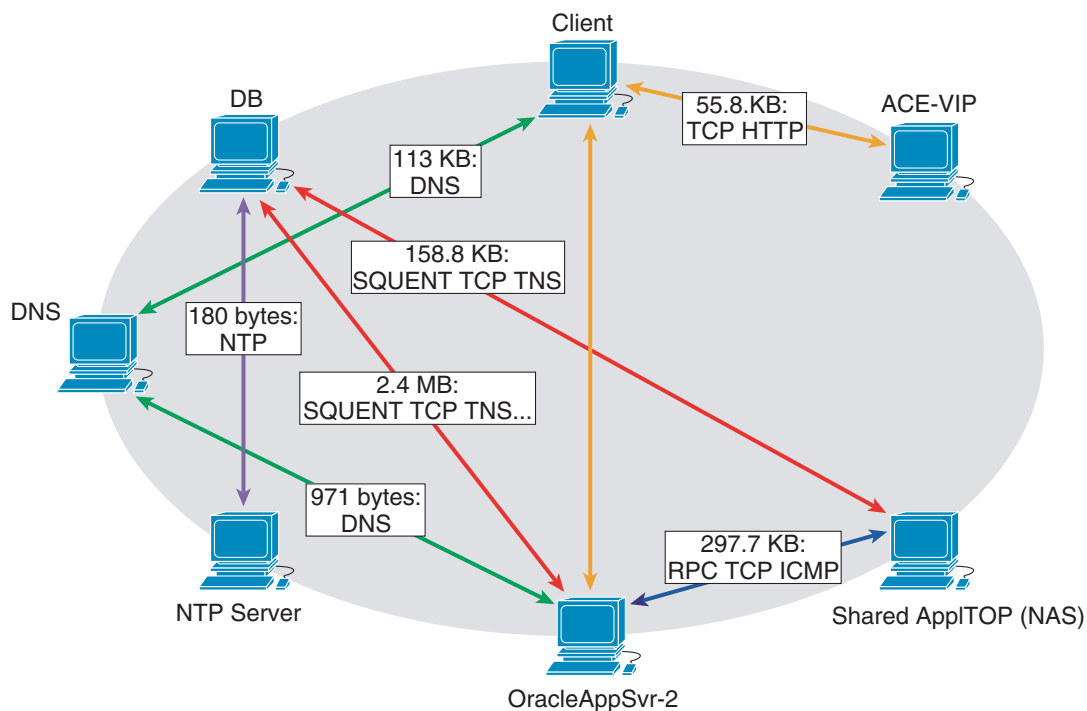
The management aspect of the data center and store network environments is critical to the success of the retail enterprise infrastructure. In the test bed, the following Cisco management tools were used to monitor and configure the network environment:

- Cisco Application Networking Manager (ANM) to monitor and manage the ACE module
- Cisco Fabric Manager for the SAN configurations
- Cisco Network Analysis Module (NAM)
- Cisco Application Analysis Solution (AAS)

Although discussing each of these tools in depth is beyond the scope of this document, the Cisco Application Analysis Solution offers a unique perspective of the Oracle enterprise application.

[Figure 22](#) is a screen shot of the AAS tool representing the network traffic generated by the initial login request of a remote store user. The AAS tool is able to resolve and recreate the logical topology of the environment, including the ACE VIP, as application relevant conversations occur between the client, server, and VIP. In addition, the protocols in use, DNS, TNS, and HTTP, are detailed as well as the traffic volume created by each flow in the Oracle application environment. The application insight afforded through the AAS toolset proved to be invaluable for understanding the complete Oracle environment.

Figure 22 Cisco Application Analysis Solution E-Business Suite Example



Note

For more information on these and other management solutions, see the following URL:
<http://www.cisco.com/en/US/products/sw/netmgts/index.html>

Performance Observations

This section describes performance testing conducted using the Oracle E-Business suite application environment. The tests were conducted using the Mercury LoadRunner application test tool. Two LoadRunner scripts were created to determine the potential benefits of the Cisco WAAS solution in an Oracle E-Business deployment. The data center and store environments described earlier provide the end-to-end network connectivity, while netem, a Fedora WAN simulation tool, injects selected delays for each five-minute test iteration. These tests simulate a store user accessing applications homed in the data center.

Figure 23 illustrates the average performance impact of delay on a non-optimized native WAN, and the improvements provided with the Cisco WAAS solution. The range of WAN delays introduced can be described as continental, transatlantic, or satellite in nature. As the chart in **Figure 23** illustrates, delay has a negative impact on the user experience. The number of successful transactions is significantly reduced as the delay is increased, and the store user is further removed from the data center application. The WAAS solution provides an improved store user experience, as indicated by the number of successful transactions.

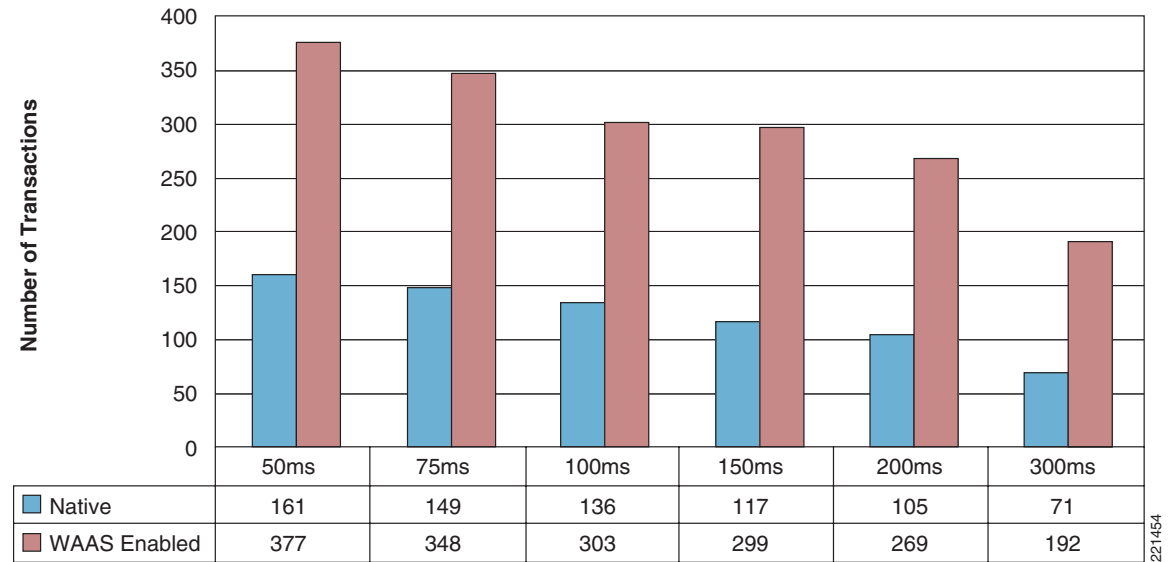
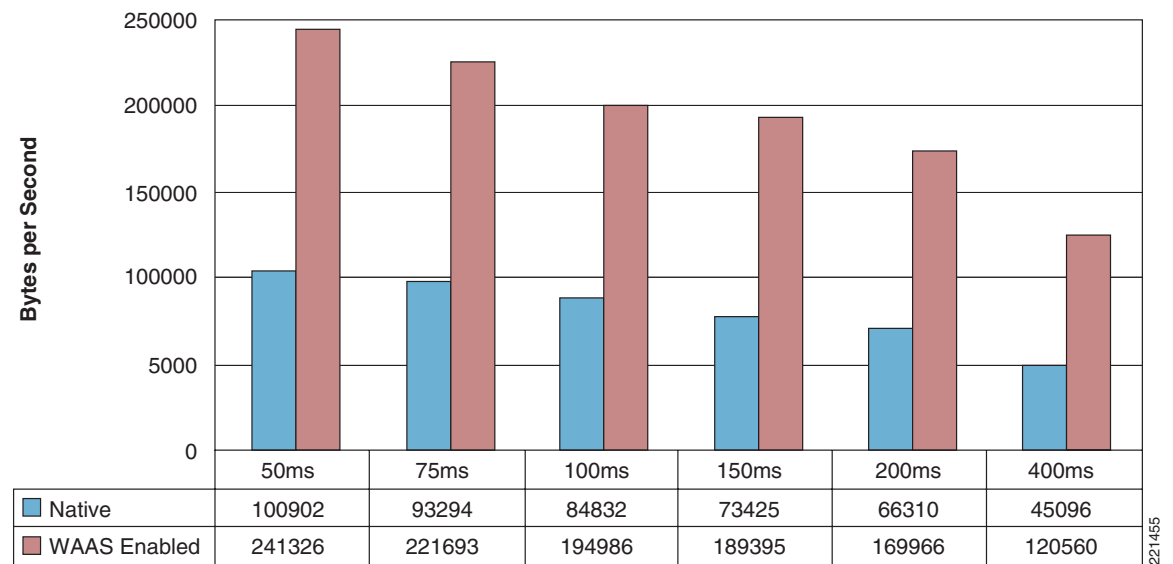
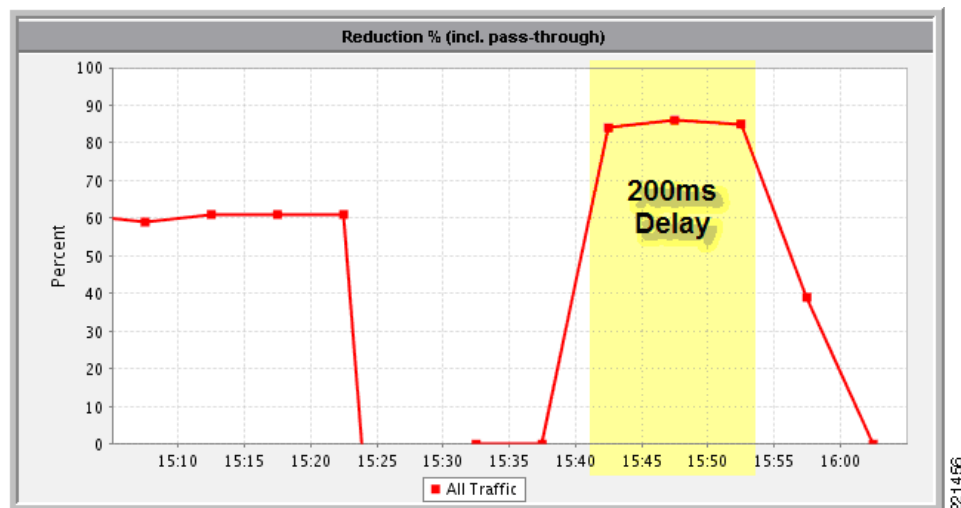
Figure 23 *iProcurement Transaction Summary*

Figure 24 shows the average amount of data received by the LoadRunner virtual client in the store. The use of DRE and compression technologies on the WAE devices allow for this LAN-like user experience, even across 400 ms WAN delays.

Figure 24 *iProcurement Throughput Summary*

The WAE devices also show the performance gains via the Central Manager (CM) GUI. The WAE CM shows that WAN traffic reduction is the 80–90 percent range. This effectively means that the amount of bandwidth required to support the E-Business application environment is reduced.

Figure 25 is a view of the WAE CM reflecting the traffic reduction on the WAN.

Figure 25 WAE Central Manager Traffic Reduction Sample with 200 ms of WAN Delay

The CLI commands on the WAEs provides further insight to the application optimizations occurring across the retail network. Figure 26 is a snapshot of the **show statistics dre detail** command executed on the store WAE.

Figure 26 Sample of DRE Statistics

```

Encode:
  Overall: msg:      2341, in:   1802 KB, out:   455 KB, ratio:  74.75%
         DRE: msg:      2341, in:   1802 KB, out:  1337 KB, ratio:  25.81%
DRE Bypass: msg:      0, in:     0 B
         LZ: msg:      2331, in:  1337 KB, out:   454 KB, ratio:  65.98%
LZ Bypass: msg:      10, in:    243 B
  Avg latency:      0.211 ms
  Message size distribution:
    0-1K=91% 1K-5K=8% 5K-15K=0% 15K-25K=0% 25K-40K=0% >40K=0%
Decode:
  Overall: msg:      6276, in:   3118 KB, out:  40174 KB, ratio:  92.24%
         DRE: msg:      6274, in:  13680 KB, out:  40170 KB, ratio:  65.94%
DRE Bypass: msg:      2, in:    4218 B
         LZ: msg:      5494, in:  2978 KB, out:  13544 KB, ratio:  78.01%
LZ Bypass: msg:      782, in:   140 KB
  Avg latency:      0.224 ms
  Message size distribution:
    0-1K=37% 1K-5K=13% 5K-15K=37% 15K-25K=8% 25K-40K=2% >40K=0%

```

In this example, you can see that the WAE has received 2341 messages from the store users totaling 1802 KB, and has reduced and compressed the amount of traffic crossing the WAN via DRE and LZ compression to 455 KB, a nearly 75 percent savings. From the data center servers, the WAE has received 6276 messages totaling 3118 KB. Through decompression and DRE reconstruction, the WAE has pushed 40,174 KB toward the remote users in the store, optimizing nearly 92 percent of the traffic.

Summary and Conclusions

The Cisco Lean Retail Oracle E-Business Suite solution provides best practices and implementation guidance that optimizes application availability, performance, and security while lowering application ownership costs.

Cisco Application Networking Services, featuring the Cisco Application Control Engine and Wide Area Application Services product families provides data center, retail store, and the store associate an improved application experience while centralizing the application components. The performance test results reveal the benefits of deploying application network services in an Oracle application environment.

As the retailer expands around the globe and applications evolve to meet the ever-increasing demands of retail, network administrators should leverage the use of application optimization services in the network to keep services in the data center while providing LAN like performance to the stores.

Appendix A—Configurations

Oracle E-Business Suite requires modifications to the APPL_TOP tier to employ network-based load balancing and SSL offload services. The autoconfiguration file retains the APPL_TOP tier configuration information and must be modified to support these advanced services. A previously released document, *Integrating Oracle E-Business Suite 11i in the Cisco Data Center*, details the modifications necessary to support the following network services in an E-Business suite 11i environment:

- HTTP load balancing
- Forms listener servlet
- SSL acceleration

ACE Configuration

ACE Admin Context

```
logging enable
logging trap 5
logging host 172.26.x.x udp/514

login timeout 0
hostname dc03-ace
boot system image:c6ace-t1k9-mz.3.0.0_A1_4.bin

resource-class oracle11i
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource sticky minimum 20.00 maximum unlimited

access-list everyone line 10 extended permit icmp any any
access-list everyone line 20 extended permit ip any any

class-map type management match-any ANM_management
  3 match protocol snmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol icmp any
```

```

7 match protocol https any
8 match protocol http any

policy-map type management first-match ANM_management
class ANM_management
    permit

interface vlan 146
description Management Address
ip address 172.26.x.x 255.255.254.0
peer ip address 172.26.x.x 255.255.254.0
access-group input everyone
service-policy input ANM_management
no shutdown

ft interface vlan 13
ip address 13.13.13.1 255.255.255.0
peer ip address 13.13.13.2 255.255.255.0
no shutdown

ft peer 1
heartbeat interval 200
heartbeat count 10
ft-interface vlan 13
ft group 1
peer 1
priority 150
peer priority 110
associate-context Admin
inservice

ip route 0.0.0.0 0.0.0.0 172.26.x.x

context oracle11i
description ** Context for Oracle11i Environment **
allocate-interface vlan 120
allocate-interface vlan 146
allocate-interface vlan 220
allocate-interface vlan 320
member oracle11i

ft group 2
peer 1
priority 150
peer priority 110
associate-context onearm
inservice

ft group 3
peer 1
priority 150
peer priority 110
associate-context oracle11i
inservice

```

ACE Oracle11i Context

Generating configuration....

```

access-list ALLOW_TRAFFIC line 8 extended permit icmp any any
access-list ALLOW_TRAFFIC line 32 extended permit ip any any
access-list ALLOW_TRAFFIC line 40 extended permit tcp any any

```

```

probe http HTTP_PROBE
  description This is a basic HTTP Probe
  port 8000
  interval 5
  passdetect interval 5
  passdetect count 5
  expect status 200 200
probe icmp WAE
  interval 5
  passdetect interval 3
  passdetect count 5

parameter-map type http TCP-reuse
  server-conn reuse

rserver host DC01-ESE-WCE2
  description DC01-ESE-WCE2
  ip address 10.220.1.100
  inservice
rserver host DC01-ESE-WCE3
  description DC01-ESE-WCE3
  ip address 10.220.1.103
  inservice
rserver host DC02-WAE7326-2
  description Data Center WAE#2
  ip address 10.220.1.102
  inservice
rserver host OracleNode1
  description Oracle APPL_TOP Node
  ip address 10.20.100.101
  inservice
rserver host OracleNode2
  description Oracle APPL_TOP Node
  ip address 10.20.100.102
  inservice
rserver host OracleNode3
  description Oracle APPL_TOP Node
  ip address 10.20.100.103
  inservice
rserver host WebCache1
  description Standalone Oracle WebCache
  ip address 10.42.100.101
  inservice

! The APPL_TOP servers listen on port 8000 by default.
serverfarm host APPL_TOP_FARM
  description This is the APPL_TOP server farm.
  probe HTTP_PROBE
  rserver OracleNode1 8000
    inservice
  rserver OracleNode2 8000
    inservice
  rserver OracleNode3 8000
    inservice

serverfarm host WAE-SERVERS
  transparent
  probe WAE
  rserver DC01-ESE-WCE2
    inservice
  rserver DC01-ESE-WCE3
    inservice
  rserver DC02-WAE7326-2

```

```

inservice

! HTTP cookie sticky is employed for the APPL_TOP farm
sticky http-cookie ACEOptimized sticky-ace-cookie
  cookie insert browser-expire
  replicate sticky
  serverfarm APPL_TOP_FARM

! Allowed management traffic
class-map type management match-any ANM_MANAGEMENT
  3 match protocol snmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol icmp any
  7 match protocol https any
  8 match protocol http any

! Oracle APPL_TOP VIP address
class-map match-all ORACLE_VIP
  2 match virtual-address 10.20.100.100 tcp eq www

! Permit ANM_MANAGEMENT class traffic
policy-map type management first-match ANM_MANAGEMENT
  class ANM_MANAGEMENT
    permit

! This policy references the sticky server farm created to support the APPL_TOP servers
policy-map type loadbalance first-match ORACLE_POLICY
  class class-default
    sticky-serverfarm sticky-ace-cookie
! Insert the source IP address of the client for logging purposes when TCP reuse enabled
    insert-http X-forwarder header-value "%is"

! This sends traffic the WAE farm
policy-map type loadbalance first-match WAE_TRAFFIC
  class class-default
    serverfarm WAE-SERVERS

! This policy is enforced when the destination address is the Oracle APPL_TOP VIP. This
policy will forward traffic to the WAE farm via the WAE_TRAFFIC policy.
policy-map multi-match ORACLE_TCP_TRAFFIC
  class ORACLE_VIP
    loadbalance vip inservice
    loadbalance policy WAE_TRAFFIC
    loadbalance vip icmp-reply

! This policy map is enforced when the destination is the Oracle VIP (10.20.100.100).
Traffic matching that destination has the ORACLE_POLICY applied. This policy references
the sticky APPL-TOP farm
policy-map multi-match VIP_ORACLE_POLICY
  class ORACLE_VIP
    loadbalance vip inservice
    loadbalance policy ORACLE_POLICY
    loadbalance vip icmp-reply

! Globally allow traffic to the ACE interfaces
access-group input ALLOW_TRAFFIC

! This is the "south" or server facing interface. In this deployment the FWSM is deployed
transparently between the ACE and the Oracle APPL_TOP servers.
interface vlan 120
  description ** FW Facing Server Side VLAN **
  ip address 10.20.1.2 255.255.0.0

```

```

! Default gateway for the APPL_TOP farm
alias 10.20.1.1 255.255.0.0
peer ip address 10.20.1.3 255.255.0.0
mtu 2000
! ACE is acting as a load balancer
no normalization
fragment min-mtu 68
no icmp-guard
no shutdown
ip route inject vlan 320

! Management interface
interface vlan 146
ip address 172.x.x.x 255.255.254.0
peer ip address 172.x.x.x 255.255.254.0
no icmp-guard
! Allow ANM access vis this service policy
service-policy input ANM_MANAGEMENT
no shutdown

! VLAN supporting the WAE farms
interface vlan 220
description ** WAE Farm **
ip address 10.220.1.2 255.255.0.0

! Default gateway for WAEs in the farm
alias 10.220.1.1 255.255.0.0
peer ip address 10.220.1.3 255.255.0.0
mtu 2000
no normalization
fragment min-mtu 68

! Mac sticky will allow for transparent stickiness to the WAE device farm
mac-sticky enable
no icmp-guard

! This service policy supports the Oracle VIP 10.20.100.100
service-policy input VIP_ORACLE_POLICY
no shutdown
! Advertise the VIP to the network external to the data center. This route advertisement
is received by the data center aggregation layer MSFC's. OSPF and BGP update the store
ISRs.
ip route inject vlan 320

! Client facing interface
interface vlan 320
description Client Side VLAN
ip address 10.80.1.4 255.255.0.0

! Allow TCP Options to permit WAE auto-discovery
ip options allow
alias 10.80.1.6 255.255.0.0
peer ip address 10.80.1.5 255.255.0.0
mtu 2000

! ACE is configured as a load balancer
no normalization
fragment min-mtu 68
no icmp-guard

! Service policy applied to ingress traffic in this case requests to the VIP 10.20.100.100
are intercepted and optimized via the WAE serverfarm
service-policy input ORACLE_TCP_TRAFFIC
no shutdown

```

```

!Default Route to HSRP Address on the Aggregation Catalyst 6500's MSFC
ip route 0.0.0.0 0.0.0.0 10.80.1.1

snmp-server contact "xxxxx@cisco.com"
snmp-server location "RTP, NC"
snmp-server community MyCommunity group Network-Monitor
snmp-server community public group Network-Monitor

snmp-server host 172.x.x.x traps version 1 public
snmp-server host 172.x.x.x traps version 3 auth admin
snmp-server trap-source vlan 146

snmp-server enable traps slb vserver
snmp-server enable traps slb real
snmp-server enable traps syslog
snmp-server enable traps snmp authentication
snmp-server enable traps snmp linkup
snmp-server enable traps snmp linkdown

```

WAE Configuration

```

! WAAS version 4.0.9 (build b10 Apr  6 2007)
!
device mode application-accelerator
!
!
hostname DC02-WAE7326-2
!
primary-interface GigabitEthernet 1/0
!
!
!
interface GigabitEthernet 1/0
ip address 10.220.1.102 255.255.0.0
exit
interface GigabitEthernet 2/0
ip address 172.x.x.x 255.255.254.0
exit
!
!
!This is the alias address on the ACE device
ip default-gateway 10.220.1.1
!
no auto-register enable
!
ntp server 10.220.99.99
!
central-manager address 192.168.1.33
cms enable
!
!
!
tfo tcp optimized-send-buffer 8192
tfo tcp optimized-receive-buffer 8192
!
!
adapter epm enable
!
! The APPL_TOP traffic is traversing the WAN using port 80. The default policy configured
on the WAE will be applied. Note that the APPL_TOP configuration can be modified to any
port.

```

```

policy-engine application
  classifier HTTP
    match dst port eq 80
    match dst port eq 8080
    match dst port eq 8000
    match dst port eq 8001
    match dst port eq 3128
  name Web
...
! Full optimization is applied to the APPL_TOP WAN traffic
  map basic
    name Web classifier HTTP action optimize full

!
!
! End of WAAS configuration

```

Appendix B—References

- Application Networking Services documentation—
http://www.cisco.com/en/US/products/hw/contnetw/tsd_products_support_category_home.html
- Oracle Metalink document ID 233428.1—*Sharing the Application Tier File System in Oracle Applications 11i*
<https://metalink.oracle.com/metalink/plsql/showdoc?db=NOT&id=233428.1>
- Oracle Metalink document ID 217368.1—*Advanced Configurations and Topologies for Enterprise Deployments of E-Business Suite 11i*
<https://metalink.oracle.com/metalink/plsql/showdoc?db=NOT&id=217368.1>
- Oracle Metalink document ID 233428.1—*Using Forms Listener Servlet with Oracle Applications 11i*
<https://metalink.oracle.com/metalink/plsql/showdoc?db=NOT&id=233428.1>
- Oracle Applications 11i (11.5.10.2) Documentation Library—
http://download-east.oracle.com/docs/cd/B25516_08/current/html/docset.html

Appendix C—Glossary

Term	Definition
Cisco Application Control Engine (ACE)	The Cisco Application Control Engine is a module within the Catalyst 6500 Series switch that allows applications resources to be distributed and managed via logical groups within a given physical platform. The ACE also provides high levels of Layer 4–7 performance (16 Gbps and 345,000 connections per second) to optimize application performance and provide scalability. For more information on the ACE service module see the following URL: http://www.cisco.com/en/US/products/ps6906/index.html
Cisco Firewall Services Module (FWSM)	The Cisco Firewall Services Module (FWSM) is a high-speed, integrated firewall module for Cisco Catalyst 6500 Series switches and Cisco 7600 Series routers, and provides the fastest firewall data rates in the industry: 5-Gbps throughput, 100,000 CPS, and 1M concurrent connections. Up to four FWSMs can be installed in a single chassis, providing scalability to 20 Gbps per chassis. For more information on the FWSM service module, see the following URL: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
Cisco Wide Area Application Engine (WAE)	The Cisco Wide Area Application Engine (WAE) platforms are a portfolio of powerful, scalable network appliances that host WAN optimization and application acceleration solutions that enable store server consolidation, performance improvements for centralized applications, and provide remote users with LAN-like access to applications, storage, and content across the WAN.
Cisco WAAS Central Manager	Cisco WAAS is centrally managed by a scalable, secure, and simple function called the Cisco WAAS Central Manager that runs on Cisco WAE appliances. The central manager can be configured for high availability by deploying a pair of Cisco WAEs as central managers; configuration and monitoring data is automatically shared by the two central manager WAEs. The central manager provides a centralized mechanism for configuring features and reporting, and can manage a topology containing thousands of Cisco WAE nodes.